PUBLIC

CALL FOR AN EXPRESSION OF INTEREST FOR A SECONDED NATIONAL EXPERT
Ref. eu-LISA/26/SNE/3.1

Post:	Security Expert – Security Policy and Coordination
Sector/Unit:	Security Policy and Coordination Sector / Security Unit
Status:	Seconded National Expert (SNE)
Location:	Tallinn, ESTONIA
Starting date:	as soon as possible
Duration of secondment:	2 years with the possibility to renew if in the interest of eu-LISA
Level of Security Clearance:	SECRET UE/EU SECRET [1]
Closing date for applications	**31 July 2026 at 23:59 EEST** (Eastern European Summer Time) and 22:59 CEST (Central European Summer Time)[2]

[1] Decision of the Agency Management Board, nr 2019-273, setting the Security Rules for Protecting EU Classified Information in eu-LISA
[2] Date of publication: 18/06/2026

1. INFORMATION ABOUT THE AGENCY

We are eu-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. We are proud to design, develop and operate large-scale information systems at the heart of Schengen, in the area of internal security, border management and judicial cooperation.

Our core mission is to keep Europe safe through technology, operating IT systems and providing services related to EU Justice and Home affairs policies. We aim to help the EU Citizens feel safe, protected, free, fairly treated and part of a united Europe.

Join us to become part of our organisational culture, an inclusive and diverse people centric environment. We believe in “Together as one, we are making it happen”. We want our people to feel respected, valued and empowered. With a workforce consisting of more than 24 different nationalities, we embrace the international work environment and collaborate with colleagues from diverse backgrounds. It is our policy to provide equal employment opportunities for all applicants regardless of gender, race, disability, age, religion or belief, political views, sexual orientation, marital status or family situation, language, social origin, ethnicity or being part of a national minority.

We believe in creating a positive and enjoyable work environment for our people and we take pride in nurturing a work environment that values and recognises the contributions of our team members. As an organisation, we understand the importance of employee recognition in driving motivation and creating a fulfilling workplace.

Please visit our website and discover more about eu-LISA’s core activities.

2. THE SECURITY UNIT

The Security Unit (SCU) is responsible for safeguarding eu-LISA’s assets, including the large-scale IT systems, infrastructure, premises and data entrusted to the Agency. By ensuring an appropriate level of security, resilience and continuity for the Agency’s operations, SCU supports the secure and uninterrupted functioning of large-scale IT systems in the area of Justice and Home Affairs (JHA), in line with eu-LISA’s mandate under Article 2 of its Establishing Regulation.

To support continuous service availability for the EU JHA community, SCU’s activities cover security governance and assurance, security risk management, information security, cyber security, business continuity, disaster recovery, protective security and the protection of classified information.

SCU comprises four sectors: (1) Security Policy and Coordination Sector (SPCS); (2) Information Security and Resilience Sector (ISRS); (3) Cyber Security Sector (CYBS); (4) Protective Security Sector (PSCS).

- The Security Policy and Coordination Sector (SPCS) is responsible for the governance, coordination and continuous improvement of eu-LISA's security framework. It develops, coordinates and monitors the implementation of security policies, procedures, standards and controls, and supports the consistent application of security requirements across the Agency. The Sector contributes to security planning, reporting, assurance activities, risk coordination, awareness-raising and cooperation with internal and external stakeholders. It also supports the effective operation and evolution of the Security and Continuity Management System (SCMS), ensuring alignment between strategic security objectives, regulatory requirements and operational security needs.

- The Information Security and Resilience Sector (ISRS) is responsible for information security management, security assurance, business continuity and disaster recovery. It provides assurance and resilience services for eu-LISA's corporate and JHA information systems and services, as well as for the underlying infrastructure hosting them, with the objective of supporting secure, reliable and uninterrupted operations.

- The Cyber Security Sector (CYBS) is responsible for protecting eu-LISA's digital assets, including eu-LISA's corporate and JHA information systems, infrastructure and data entrusted to the Agency. It ensures cyber security monitoring, detection, analysis and response capabilities, with the objective of preserving the confidentiality, integrity and availability of systems and services managed by eu-LISA.

- Protective Security Sector (PSCS) is responsible for is responsible for protective and physical security measures across eu-LISA's sites. It ensures the protection of premises, staff, visitors, assets and classified information, including through access control, physical security procedures, security incident handling, and the implementation of relevant protective security requirements.

The Unit is located in Tallinn, ESTONIA, and Strasbourg, FRANCE.

3. THE SECONDMENT

SNEs are seconded to eu-LISA according to the Decision No 2012-025 of the Management Board of eu-LISA as of 28 June 2012.

SNEs should enable eu-LISA to benefit from the high level of their professional knowledge and experience, in particular in areas where such expertise is not readily available.

The SNEs employer shall undertake to continue to pay his/her salary, to maintain his/her administrative status throughout the period of the secondment. The SNEs employer shall also continue to be responsible for all his/her social rights, particularly social security and pension.

SNEs shall assist eu-LISA's statutory staff members. They may not perform middle or senior management duties, even when deputising for their immediate superior. Under no circumstances may an SNE on his/her own represent the Agency with a view to entering into commitments, whether financial or otherwise, or negotiating on behalf of eu-LISA.

The SNE shall carry out the duties and conduct his/her tasks solely within the interests of eu-LISA. He/she shall neither seek nor take instruction from any government, authority, organisation nor person outside the Agency. He/she shall carry out the duties assigned objectively, impartially and in keeping with his/her duties of loyalty to the EU.

The initial period of the secondment may not be less than six months nor more than two years. It may be renewed once or more, up to a total period not exceeding four years, at the request of eu-LISA.

Exceptionally, at the request of the concerned Head of Unit and where the interest of the service warrants it, the Executive Director of eu-LISA may authorise one or more extensions of the secondment for a maximum of two more years at the end of the four-year period.

The secondment is authorised by the Executive Director and effected by an exchange of letters between the Executive Director and the Permanent Representation of the Member State concerned, the associated country's mission to the EU or the intergovernmental organisation (IGO).

The SNE is entitled, throughout the period of the secondment, to a daily subsistence allowance and a monthly subsistence allowance, applicable to the place of secondment.

The selected applicant will need to have, or be in a position to obtain, a valid Personnel Security Clearance Certificate (SECRET UE/EU SECRET). A Personnel Security Clearance Certificate (PSCC) means a certificate issued by a competent authority establishing that an individual is security cleared and holds a valid national or EU PSC, which shows the level of EU Classified Information (EUCI) to which that individual may be granted access, the date of validity of the relevant PSC and the date of expiry of the certificate itself. For more information about EUCI please consult the Decision of the Agency Management Board, nr 2019-273, setting the Security Rules for Protecting EU Classified Information in eu-LISA[3].

Applicants, who currently hold a valid security clearance, shall provide a copy of the security clearance to eu-LISA and specify the issuing authority, level and date of expiry. In case the validity of the security clearance expires within six months, the renewal procedure to be initiated expeditiously. For applicants,

[3] https://www.eulisa.europa.eu/AboutUs/Documents/MB%20Decissions/2019-273_EUCI%20rules.pdf

who do not hold a security clearance, the procedure will be initiated expeditiously by eu-LISA. Failure to obtain the required security clearance certificate from the National Security Authority during the secondment, will give the right to eu-LISA to terminate the secondment.

4. TASKS AND RESPONSIBILITIES

Reporting to the Head of the Security Unit and under the supervision of the Head of Security Policy and Coordination Sector, the Security Expert will support the Sector in maintaining and consolidating eu-LISA's security policy and governance framework. The post aligns that framework with the evolving regulatory baseline and integrates it coherently across Agency-level documentation, security risk coordination, audit follow-up, and the governance and accreditation of sensitive or classified systems.

The Security Expert will be responsible for:

- supporting the review, structuring and maintenance of security policies, procedures, standards, guidelines and operating instructions, ensuring consistency with applicable security obligations and related Agency-level documentation;
- contributing to the governance and accreditation of systems handling sensitive or classified information, including coordination of inputs, preparation of supporting documentation, follow-up of requirements and maintenance of traceability between decisions, controls and evidence;
- contributing to the implementation of the evolving security regulatory baseline through requirement mapping, gap analysis, action planning, stakeholder coordination and follow-up;
- supporting security governance processes, including the preparation of briefings, reports, agendas, minutes, decision points, action trackers and inputs for management or governance bodies;
- supporting audit and assessment readiness by coordinating evidence collection, recommendations, management responses, action plans and follow-up of agreed measures;
- supporting security awareness-raising activities and cooperation with internal and external stakeholders in relation to the security framework.

5. QUALIFICATIONS AND EXPERIENCE REQUIRED

5.1. Eligibility criteria

Applicants will be considered eligible for the selection based on the following formal criteria to be fulfilled by the deadline for applications:

- to be a national of one of the Member States of the European Union, Norway, Iceland, Liechtenstein or Switzerland and enjoy the full rights as a citizen;
- to be employed by a national, regional or local public administration or an Inter-Governmental Organisation (`IGO`);

- to have worked for the employer on a permanent or contractual basis for at least 12 months before the secondment and shall remain in service of the employer throughout the period of secondment;
- to have a thorough knowledge of one of the European Union languages and a satisfactory knowledge of another European Union language to the extent necessary for the performance of the duties. SNE from non-member country must produce evidence of a thorough knowledge of one European Union language necessary for the performance of his/her duties.

Only duly documented professional activity is taken into account. In case of part-time work, the professional experience will be calculated pro-rata in line with the workload stated by the applicant.

Compulsory military service or equivalent civilian service shall be taken into consideration as professional experience if the official documentation is provided.

5.2. Selection criteria

Suitability of applicants will be assessed against the following criteria in different steps of the selection procedure.

5.2.1. ***Professional experience and knowledge:***

The applicant will be required to demonstrate that he/she has:

- a University Degree (minimum of three (3) years) in Computer Science, Law, Public Administration, European Affairs or another field relevant to the tasks of the Agency;
- proven relevant professional experience of at least three (3) years in security governance, information security, security risk management, security accreditation or a closely related field (for details please refer to section 4);
- excellent drafting and presenting skills in English, both orally and in writing, at least at level C1;
- experience in developing, maintaining or improving a security management system, information security management system, or business continuity management system;
- experience in managing management-system documentation and records, including policies, procedures, controls, registers, implementation evidence and periodic reviews;
- knowledge of security risk coordination, including risk assessment, treatment, monitoring, escalation, residual-risk considerations and related governance records;
- familiarity with security audit and assurance coordination, including evidence collection, recommendation follow-up, management responses and action tracking;
- experience in the governance, security accreditation, security authorisation or approval-to-operate of communication and information systems handling sensitive non-classified information or EU classified information.

5.2.2. ***Besides the following attributes would be advantageous:***

- knowledge of Regulation (EU, Euratom) 2023/2841 and COM(2022) 119 final / 2022/0084(COD), Proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union;

- knowledge of Council Decision 2013/488/EU, Commission Decision (EU, Euratom) 2015/444 and/or equivalent national rules on classified information;
- knowledge of relevant GRC, security, risk, business continuity or internal control frameworks, such as ISO/IEC 27001, ISO/IEC 27005, ISO 22301, NIST, COBIT or equivalent frameworks;
- experience working with EU institutions, bodies or agencies, national administrations, national security authorities, law enforcement authorities or stakeholders in the Justice and Home Affairs area.

*5.2.3. **Personal qualities***

Attributes especially important to this post include:

- Strong oral and written communication and interpersonal skills, with the ability to convey complex security, governance and regulatory matters clearly, accurately and unambiguously to different audiences;
- Strong organisational skills, ability to maintain oversight of multiple workstreams, prioritize effectively and meet tight deadlines ensuring attention to detail;
- Sound judgement, discretion and reliability when handling sensitive matters, security-related information and interactions with internal and external stakeholders;
- Ability to coordinate processes and stakeholders in a multicultural environment, promoting cooperation, clarity of roles and timely follow-up of agreed actions;
- Initiative and results orientation, including the ability to identify improvements, propose practical solutions and support the continuous improvement of processes and procedures;
- Resilience and adaptability, with the ability to remain focused, objective and effective under pressure and in a rapidly evolving work environment.

6. EQUAL OPPORTUNITIES

eu-LISA applies an equal opportunities policy and accepts applications without distinction on grounds of sex, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

7. SELECTION PROCEDURE

The selection procedure includes the following steps:

- Selection Committee designated by the Appointing Authority (eu-LISA`s Executive Director) is set up for the selection procedure;
- After registration, each application is checked to verify whether the applicant meets the eligibility criteria;
- All eligible applications are evaluated by the Selection Committee based on the selection criteria defined in the open call;
- The best-qualified applicants, who obtained the highest number of points, are short-listed for an interview, which may be complemented by a written competency test[4];

[4] The Selection Committee has the discretion to choose between remote and on-site interviews/tests as deemed appropriate. For remote interviews, the Selection Committee reserves the right to conduct the interview using an online video interviewing tool for synchronous and/or asynchronous (e.g., recorded) interviews.

- The interview and written test are conducted in English. In case English is a mother tongue of an applicant, some interview or test questions may be held in language indicated by the applicant on the application form as the 2nd EU language;
- During the interview and the written test, the Selection Committee examines the profiles of applicants and scores the applicants in accordance with the selection criteria;
- After the interviews and tests, the Selection Committee draws up a non-ranked list of the most suitable candidates to be included on a reserve list for the post and proposes it to the Appointing Authority. The Selection Committee may also propose to the Executive Director the best suitable applicant to be offered secondment for the post;
- The Appointing Authority choses from the reserve list an applicant to whom to offer the secondment;
- Applicants put on the reserve list may also be used for secondment to a similar post depending on the needs of the eu-LISA and budgetary situation as long as the reserve list is valid;
- The reserve list established for this selection shall be valid **until 31 December 2027** (the validity period may be extended);
- Each applicant invited for an interview will be informed whether or not he/she has been placed on the reserve list. **Applicants should note that inclusion on a reserve list does not guarantee a secondment by eu-LISA.**

The Selection Committee's work and deliberations are strictly confidential and any contact with its members is strictly forbidden.

Because English is the working language of eu-LISA and because the successful applicant will be requested to immediately be operational, the selection procedure will be performed in English and all communication with applicants will be held in English.

8. PROTECTION OF PERSONAL DATA

eu-LISA ensures that applicants' personal data is processed in accordance with Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data[5].

The purpose of processing personal data is to enable selection procedure.

[5] Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018, OJ L 295, 21.11.2018, p. 39

The selection procedure is conducted under the responsibility of the eu-LISA's Human Resources Unit (HRU), within the Corporate Services Department. The controller for personal data protection purposes is the Head of HRU.

The information provided by the applicants will be accessible to a strictly limited number of staff members of the HRU staff, to the Selection Committee, and, if necessary, to the Executive Director, Security and/or the Legal Officer of eu-LISA.

Almost all fields in the application form are mandatory; the answers provided by the applicants in the fields marked as optional will not be taken into account to assess their merits.

Processing begins on the date of receipt of the application. Our data storage policy is as follows:

- for applications received but not selected: the paper dossiers are filed and stored in archives for 2 years after which time they are destroyed;
- for applicants placed on a reserve list but not recruited: data is kept for the period of validity of the reserve list + 1 year after which time it is destroyed;
- for recruited applicants: data is kept for a period of 10 years as of the termination of employment or as of the last pension payment after which time it is destroyed.

All applicants may exercise their right of access to and right to rectify personal data. In the case of identification data, applicants can rectify the data at any time during the procedure. In the case of data related to the admissibility criteria, the right of rectification cannot be exercised after the closing date of applications' submission.

Any substantiated query concerning the processing of his/her personal data can be addressed to HRU at eulisa-SNEPOSTING@eulisa.europa.eu

Applicants may have recourse at any time to eu-LISA`s Data Protection Officer (dpo@eulisa.europa.eu) and/or the European Data Protection Supervisor (edps@edps.europa.eu).

9. APPLICATION PROCEDURE

In order for application to be valid and considered eligible, the applicant is required to submit:

- eu-LISA standard application form filled in in English and hand-signed (scanned into PDF format);
- proof of the National Administration Authorisation – Form 1A (Employer authorisation for SNE applicant), provided on eu-LISA website;
- a copy of security clearance (if available).

Applications must be sent by the Permanent Representation or a national contact point or by the associated countries competent authority or the administration of IGO to the following e-mail address

before the deadline: eulisa-SNEPOSTING@eulisa.europa.eu. Please liaise with your Permanent Representation to ensure that your application meets deadline.

The standard application form can be downloaded from eu-LISA website:
http://www.eulisa.europa.eu/JobOpportunities/Pages/SecondedNationalExpert.aspx

The closing date for submission of applications is:

- **31 July 2026 at 23:59 EEST (Eastern European Summer Time) and 22:59 CEST (Central European Summer Time).**

The subject of the e-mail should include the **title of the Open Call and Reference No eu-LISA/26/SNE/3.1.**

Incomplete applications and applications received by eu-LISA after the deadline will be disqualified and treated as non-eligible.

Applicants are strongly advised not to wait until the last day to submit their applications, since heavy internet traffic or a fault with the internet connection could lead to difficulties in submission. eu-LISA cannot be held responsible for any delay due to such difficulties.

Once the applications have been registered, applicants will receive an acknowledgement message by e-mail confirming the receipt of the application.

Please note that if at any stage of the selection procedure it is established that any of the requested information provided by an applicant is false, the applicant in question will be disqualified.

In case of any queries about the selection process, please contact through the e-mail:
eulisa-SNEPOSTING@eulisa.europa.eu.