European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

CALL FOR EXPRESSION OF INTEREST FOR SECONDED NATIONAL EXPERTS (SNES)

REF. ENISA-SNE-2020-03

1. MISSION OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

The European Union Agency for Cybersecurity (ENISA) holds a discreet and enhanced role under the mandate of the Cybersecurity Act Regulation[1]. The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, European Union institutions, industry, academia and EU citizens.

ENISA contributes to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness raising, whilst developing cross-border communities and synergies.

With this Call, ENISA asserts its interest to ensure that the 12 posts foreseen for Seconded National Experts (SNEs) in the Agency's establishment plan are fulfilled. At the publication of this call (Spring 2020) ENISA seeks to fill 5 **SNE posts** to take up duties in 2020.

Seconded National Experts should support the Agency's activities in one or more of the following areas, pursuant to Chapter II of Regulation (EU) 2019/881 - Cybersecurity Act (CSA):

- Article 5: Development and implementation of Union policy and law
- Article 6: Capacity-building
- Article 7: Operational cooperation at Union level
- Article 8: Market, cybersecurity certification and standardisation
- Article 9: Knowledge and information
- Article 10: Awareness-raising and education
- Article 11: Research and innovation
- Article 12: International cooperation

ENISA accepts applications for this call on a rolling basis, under these terms which are valid until 30 April 2022 at 22:00 CET zone[2] (included).

Place of employment: Athens, Greece[3].

2. WHAT CANDIDATES IS ENISA LOOKING FOR?

ENISA is looking for candidates that fit into one or more of the following profiles:

PROFILE A: KNOWLEDGE AND EXPERIENCE IN CYBERSECURITY

On a technical and operational level, acquired through relevant academic studies, research and/or professional experience as an analyst, officer or IT specialist in the private or in the public sector. Candidates are expected to demonstrate knowledge and experience in **one or more** of the following areas:

[1] Regulation (EU) 2019/881 - Cybersecurity Act: http://data.europa.eu/eli/reg/2019/881/oj
[2] CET: Central European Time
[3] ENISA reserves the right as per Staff Regulations to change the location of the post should it be in the interest of the service.

A.1. ICT security auditing, risk assessment and management;
A.2. ICT security policy development and implementation;
A.3. ICT security policies, specifications and best practices;
A.4. Cyber crisis management, incident handling and response, penetration testing and forensics;
A.5. Cybersecurity architectures;
A.6. Cybersecurity threat intelligence (CTI), vulnerability assessment and management;
A.7. Security and privacy engineering, including cryptography;
A.8. Trust services and digital identity management including public key infrastructure technologies;
A.9. Cybersecurity certification of products, services and processes and standards;
A.10. Cybersecurity technology research and innovation;
A.11. Cybersecurity capacity building, education and training;
A.12. Network and application security, including security of electronic communications, software and systems.

PROFILE B: SECTORIAL ICT TECHNICAL OR ICT POLICY KNOWLEDGE AND EXPERIENCE, AND PROVEN PROFESSIONAL UNDERSTANDING OF CYBERSECURITY ISSUES

In one or more sectors or policy fields (e.g. transport, energy, telecommunications, financial services, utilities, health, digital services, emerging technologies etc.) or in the digital economy and society, acquired through relevant academic studies, research and/or professional experience as ICT analyst, ICT specialist or ICT policy officer in the private or public sector. Candidates are expected to hold this knowledge and experience in **one or more** of the following areas:

B.1. Healthcare;
B.2. Banking and financial services;
B.3. Transport;
B.4. Energy and utilities;
B.5. Electronic government services, commerce and/or logistics;
B.6. Telecommunications;
B.7. Consumer-centred digital platforms (e.g. social media etc.);
B.8. Cloud computing;
B.9. Distributed ledgers;
B.10. Internet of Things (IoT);
B.11. Artificial Intelligence (AI);
B.12. Engineering, research and development of ICT systems and emerging technologies.

PROFILE C: GOOD BACKGROUND IN POLICY, ECONOMICS, INTERNATIONAL RELATIONS, SOCIAL SCIENCES, EU PUBLIC SECTOR, ETC. WITH A RELEVANT LINK TO CYBERSECURITY

Resulting in a proven insight and proven understanding and interest into cybersecurity, acquired through relevant academic studies, research and/or professional experience in EU or national private or public sector. Candidates are expected to hold knowledge and experience in **one or more** of the following areas:

C.1. Economics of cybersecurity;
C.2. Societal/psychological, behavioural analysis of cybersecurity;
C.3. Public policy on cybersecurity;
C.4. Cybersecurity in management information systems;
C.5. Compliance aspects of cybersecurity;
C.6. Quality management with relevance to cybersecurity;
C.7. Information assurance with relevance to cybersecurity;
C.8. Knowledge management on cybersecurity;
C.9. International relations aspects of cybersecurity;
C.10. Cybercrime investigations;
C.11. Communication, dissemination and/or awareness raising on cybersecurity;
C.12. Quantitative and qualitative methods with application on cybersecurity.

3. WHAT TASKS CAN A SNE EXPECT TO PERFORM?

The successful candidates(s) are expected to contribute to one or more of the following activities of the Agency (depending on the profile and the assignment post):

- Support EU policy development and implementation, providing advice, helping to develop technical guidelines, recommendations and tools both in general and/or in different policy and technological fields and sectors, as well as facilitating the exchange of best practices;
- Assist with information collection, sharing and analysis of cyber security incident information and relevant reports;
- Support in organising workshops and validating of findings;
- Support Member States, European Union institutions, bodies, offices and agencies to improve their capabilities on the prevention, detection, analysis of and response to cyber threats and incidents;
- Support operational communities, such as Computer Security Incident Response Teams (CSIRTs), in the area of security incident handling and response;
- Facilitate operational cooperation among Member States, European Union institutions, bodies, offices and agencies and between stakeholders, including the development and improvement of Standard Operational Procedures;
- Support the management, including crisis communication of cross-border large-scale incidents and crises (Cyber Crises Management);
- Assist the Agency's skills development and capacity building activities, such as the organisation and management of exercises, challenges, trainings etc.;
- Assist with the design, deployment and maintenance of EU cybersecurity certification schemes and the EU cybersecurity certification framework;
- Support the establishment and take-up of European and International standards for risk management and for the security of ICT products, ICT services and ICT processes;
- Support in the threat assessments and risk analysis in the area of cybersecurity, including emerging technologies;
- Support in raising public awareness of cybersecurity risks and provide guidance on good practices, in cooperation with the Member States, European Union institutions, bodies, offices and agencies and industry;
- Support European Union institutions, bodies, offices and agencies and the Member States on research needs and priorities in the field of cybersecurity;
- Support the development and maintenance of platforms related to the core operational activities;
- Support the dissemination and taking up of the results of the Agency, including engagement of relevant stakeholders;
- Take on additional tasks as required in the interest of the service.

4. WHAT ARE THE CONDITIONS OF SECONDMENT?

The framework for the Seconded National Experts (SNEs) at ENISA is defined in **Decision No MB/2013/15** of the Management Board of the European Union Agency for Cybersecurity laying down rules on the secondment of national experts (SNE) to the Agency[4]. Seconded National Experts (SNEs) are staff employed by a national, regional or local public administration who are seconded to the Agency so that it can use their expertise in a particular field. ENISA may avail of cost-free seconded national expert under certain conditions and in line with Article 2 of the MB Decision 2013/13 or SNEs for whom ENISA may pay the daily allowance and monthly subsistence allowance.

SNEs must have worked for their employer on a permanent or contract basis for at least 12 months before their secondment and shall remain in the service of that employer throughout the period of secondment. The SNE's employer shall thus undertake to continue to pay their salary, to maintain their administrative

[4] https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/decision-no-mb201315-signed.pdf

status (permanent official or contract staff member) throughout the period of secondment and to continue to be responsible for all their social rights, particularly social security and pension rights. An SNE is eligible to a daily subsistence allowance of 143.30 EUR[5] and a monthly subsistence allowance paid by ENISA. SNEs may be eligible to reimbursement of the cost of their travel between their place of origin and the place of secondment at the beginning and end of their secondment.

The initial period of secondment may not be less than six months or more than two years. It may be renewed one or more times, up to a total period not exceeding four years. Exceptionally, where the interests of the service warrant it, the Executive Director may authorise one or more extensions of the secondment for a maximum of two more years at the end of the four-year period.

5. WHAT ARE THE ELIGIBILITY CRITERIA?

To be considered eligible, candidates must satisfy all the criteria listed below:

1. Be a national of an EU Member States or of the Member States of the European Free Trade Area (EFTA), except where the Executive Director grants a derogation;
2. Have at least three years' experience of administrative or legal or scientific or technical or advisory or supervisory functions;
3. Have worked for their employer on a permanent or contract basis for at least 12 months before the secondment;
4. Remain in the service of that employer throughout the period of secondment;
5. Have a thorough knowledge of one EU language and satisfactory knowledge of a second EU official language. An SNE from a non-member state shall have thorough knowledge of one EU official language necessary for the performance of his/her duties.

6. WHAT ARE THE SELECTION CRITERIA?

All eligible candidates will be assessed against selection criteria. The selection criteria with regard to experience and knowledge (under Section 6.1) are numerically evaluated in order to identify the best-qualified candidates. Only candidates scoring above the threshold to be set by the Selection Board will be invited for an interview. Therefore, candidates are recommended to give evidence of their knowledge by specific examples and/or detailed professional experience in their application (Europass CV and Motivation letter) in order to be evaluated in the best possible way.

In addition, candidates are expected to fulfil the below behavioural competencies as outlined under section 6.2 which will be assessed during interview phase.

6.1 TECHNICAL COMPETENCIES/ SELECTION CRITERIA

1. **University diploma** in one of the following domains: Information Systems, Computer Science, Natural Science, Engineering, Management, Political Science, International Relations, Economics, Social Science or a related discipline.
2. **Relevant renowned certification**(s) would be an asset.
3. **Proven experience** in the fields brought out under the three profiles in section 2. Experience in various profiles would be an asset.
4. **Experience in contributing to or coordinating projects involving a variety of stakeholders** would be an asset.
5. **International/multicultural experience** within the areas listed under Section 2 would be an asset.
6. A thorough knowledge of **English** (minimum level required: C1 of Common European Framework of Reference for Languages, applying to each linguistic ability (speaking, writing, reading and listening)[6].

[5] Allowances are subject to correction coefficient 81.8%, which will be reviewed yearly with retroactive effect from 1 July.
[6] https://europass.cedefop.europa.eu/sites/default/files/cefr-en.pdf

6.2 BEHAVIOURAL COMPETENCIES/ SELECTION CRITERIA

7. Motivation;
8. Analysis and problem solving;
9. Priority setting, planning and organising;
10. Excellent communication skills;
11. Service-oriented and co-operative attitude.

7. WHAT ARE THE STEPS FOR THE SECONDMENT PROCEDURE?

1. Candidates send their applications (CV in Europass format and motivation letter, both documents in English) to their EU Permanent Representations;
2. Applications are forwarded by the EU Permanent Representations to ENISA;
3. The applications are screened against the eligibility and selection criteria by the Selection Board. At this stage, candidates might be asked to also fill in a self-assessment form to better map their specific fields of expertise according to the three profiles brought out in section 2;
4. The shortlisted candidates will be invited to undergo an interview. The interview will aim to assess the suitability of the candidate to perform the duties, professional knowledge and motivation. The interview will be held in English.
5. As a result of the interview, selected candidates are placed in the SNE reserve list. Inclusion in the reserve list does not guarantee recruitment. The successful candidate will be selected from the established reserve list which may also be used for the recruitment of a similar post depending on the needs of ENISA;
6. When a position becomes available, the Executive Director authorises the secondment and ENISA contacts the candidate, the Permanent Representation of the Member State concerned and/or the employer of the SNE;
7. The secondment is implemented by an exchange of letters between the Executive Director and the Permanent Representation of the Member State concerned or the employer, as the case may be. A copy of the rules applicable to SNEs at ENISA shall be attached to the exchange of letters;
8. The secondment is established by an agreement on secondment between the Executive Director, the SNE and/or his employer. A copy of this agreement is sent to the Permanent Representation of the Member State concerned.

Note: It is strictly forbidden for the candidates to make any contact with the Selection Board, either directly or indirectly. Any infringement to this rule will disqualify the candidate from the competition.

8. HOW CAN I APPLY?

In order to be considered for this position, the SNEs' Permanent Representation must send the following documents to ENISA:

- a **CV in Europass format**[7]**;**
- a Motivation letter (preferably no more than one A4 page).

ENISA accepts applications for this call on a rolling basis.

The application should be sent via the Permanent Representations of the applicants Member State (please see note below) to the following address:**sne@enisa.europa.eu**. Only complete and received within the deadline applications, will be accepted and considered further in the evaluation process.

[7] https://europass.cedefop.europa.eu/documents/curriculum-vitae.

Note: please note that ENISA only accepts applications submitted through the Permanent Representation, applications from individuals will not be accepted.

9. EQUAL OPPORTUNITIES

ENISA is an equal opportunities employer and accepts applications without distinction on the grounds of gender, racial or ethnic origin, religion or belief, age or sexual orientation, marital status or family situation. Applications from women and disabled candidates are encouraged. SNEs applications are assessed solely on the basis of their merit, and as per Staff Regulations, the Agency recruits staff on the broadest possible geographical basis from among nationals of all Member States of the European Union.

10. DATA PROTECTION

All personal data shall be processed in accordance with Regulation (EU) No 2018/1725 of the European Parliament and of the Council (OJ L 295, 21.11.2018, p. 39–98) 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. ENISA is supervised by EDPS, http://www.edps.europa.eu. For any further enquiries you may contact the Data Protection Officer at: dataprotection@enisa.europa.eu

Candidates are invited to consult the privacy statement which explains how ENISA processes personal data in relation to recruitment selection processes.

Published on ENISA's website on 06/05/2020.