Inter-Agency Mobility: Call for Applications

Cybersecurity Expert (TA/AD 5 – TA/AD 6) 2(f) - Four positions

Ref. ENISA-TA-AD-2021-05-IAM

The European Union Agency for Cybersecurity (ENISA) welcomes applications from highly motivated candidates to contribute to the development of the Agency.

ENISA is looking to draw a reserve list from which **four cybersecurity experts** will be recruited to start working in 2022, to support the Agency's activities in 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

Please send us your applications by no later than 30/08/2021 at 16:00 CET.

1. The Agency

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.

ENISA is located in Athens, Greece (the agency's official seat) with a branch office in Heraklion, Crete, Greece. In addition, ENISA is in the process of establishing a Local Office in Brussels, Belgium.

The place of employment for this vacancy is in **Athens, Greece and Brussels, Belgium[2].**

ENISA's staff are expected to be reasonably mobile in order to respond to the needs of the Member States on the basis of planned as well as ad hoc needs.

Further information about ENISA is available on the ENISA website: https://www.enisa.europa.eu/

2. Policy Development and Implementation Unit

Two Cybersecurity Experts will work in the Policy Development and Implementation Unit (PDI).

[1] Regulation (EU) 2019/881 - Cybersecurity Act: http://data.europa.eu/eli/reg/2019/881/oj

[2] The place of employment for the post within Operational Cooperation Unit is foreseen for Brussels, Belgium, while the remaining posts for Athens, Greece. ENISA reserves the right as per Staff Regulations to change the location of the post should it be in the interest of the service.

The Policy Development and Implementation Unit ensures the performance of the tasks of the Agency as set out in Art. 5 of the CSA, pursuant Article 2(2) of the MB Decision MB/2020/9. It is responsible for and leads the activities relevant to achieving the strategic objective "Cybersecurity as an integral part of EU policies" as outlined by MB/2020/8. The activities and actions undertaken by the unit within the Agency's Work Program and contribute in achieving the overall goals of the Agency as described through the recitals 1, 17, 22-24, 26, 28-30, 49 and 65 of the CSA.

The underlying mission of the unit is to facilitate and promote the consistent implementation of Union policy and law, to achieve common high level of cybersecurity of the Union's critical infrastructure and vital sectors. The work of the Unit focuses on the effective implementation of Directive (EU) 2016/1148. It also contributes to the implementation of other relevant legal instruments containing cybersecurity aspects, such as the Union policy in the field of electronic identity and trust services, security of electronic communications, and to the development of Union laws relating to data protection and privacy in order to achieve a more comprehensive, cross-policy approach to building cyber resilience.

The unit provides advice, opinions and analyses regarding all Union matters related to policy and law development, updates and reviews in the field of cybersecurity and sector-specific aspects. It will assist the Cooperation Group created by the Directive (EU) 2016/1148 in the execution of its tasks, in particular by providing expertise and advice, and by facilitating the exchange of best practices, inter alia, with regard to the identification of operators of essential services by the Member States, and in cooperation with the knowledge and information team on cross-border dependencies regarding risks and incidents

3. Capacity Building Unit

One Cybersecurity Expert will work in the Capacity Building Unit (CBU).

The Capacity Building Unit ensures the performance of the tasks of the Agency as set out in Art. 6 and Art 7(5) of the CSA, pursuant to Article 2(3) of the MB Decision MB/2020/9. It is responsible for and leads the activities relevant to achieving the strategic objective "Cutting-edge competences and capabilities in cybersecurity across the Union" as outlined by MB/2020/8. The activities and actions undertaken by the unit within the Agency's Work Program to implement this objective and contribute in achieving the overall goals of the Agency as described through the recitals 6, 9, 26, 30, 32 and 47 of the CSA.

CBU undertakes efforts to further increase the capabilities, develop skills and enhance preparedness of Member States and businesses to raise their resilience and comprehensively respond to cyber threats. With a view to increasing Union preparedness in responding to incidents, the unit should regularly organise cybersecurity exercises at Union level, and, at their request, support Member States and Union institutions, bodies, offices and agencies in organising such exercises. On a biennial basis it prepares and organises large-scale comprehensive exercises, which include technical, operational or strategic elements. In planning, preparing and organising the exercises, as well as analysing the results and making recommendations, the unit cooperates with other units and permanent teams.

The unit provides support to Member States at their request, such as by providing advice on how to improve their capabilities and preparedness to prevent, detect and respond to incidents except for those mentioned in Article 7. CBU contributes to the development and updating of strategies on the security of network and information liaise with the relevant competent authorities at the national and Union level to fulfill its mandate, in particular for the planning, preparation, organisation and follow-up of exercises and trainings.

4. Operational Cooperation Unit

One Cybersecurity Expert will work in the Operational Cooperation Unit (OCU).

The Operational Cooperation Unit (OCU) ensures the performance of the tasks of the Agency as set out in Art. 7 (except for Art 7(5)) of the CSA, pursuant Article 2(4) of the MB Decision MB/2020/9. Moreover, the unit is responsible for implementing the provisions foreseen in Article 27(4) of the CSA in the Agency. It is responsible and leads the activities relevant to achieving the strategic objective "Effective cooperation amongst operational actors within the Union in case of massive cyber incidents". The Unit contributes in achieving the overall goals of the Agency as described through the recitals 5-6, 25, 31-37, 46 of the CSA.

The Operational Cooperation Unit, in synergy with national and EU actors, undertakes efforts to support effective and coordinated responses and crisis management at Union level, building on dedicated policies and wider instruments for European solidarity and mutual assistance.

OCU helps to build and enhance capabilities and preparedness to prevent, detect and respond to large-scale cross-border cyber incidents, gather relevant information and contribute to the creation common situational awareness. It acts as a facilitator between the technical community, as well as between decision makers responsible for crisis management. The Unit supports the functioning of the CSIRTs network, operational cooperation within CSIRTs network and assists the Capacity Building Unit with the development and enhancement of CSIRTs with a view to achieving a high common level of their maturity in the Union.

The successful candidates will be required to act and abide by ENISA's core values:

- **Community Mind-Set:** ENISA works with communities, respecting their competencies and expertise, and fosters synergies and trust to best achieve its mission.
- **Excellence:** ENISA aims for state-of-the-art expertise in its work, upholds the highest quality standards of operation and evaluates its performance to strive for continuous improvement through innovation and foresight.
- **Integrity / Ethics:** ENISA upholds ethical principles and EU relevant rules and obligations in its services and working environment ensuring fairness and inclusiveness.
- **Respect:** ENISA respects fundamental European rights and values covering all its services and working environment, as well as the expectations of its stakeholders.
- **Responsibility:** ENISA assumes responsibility thus ensuring integration of the social and environmental dimensions into practices and procedures.
- **Transparency:** ENISA adopts procedures, structures and processes that are open, factual and independent, thus limiting bias, ambiguity, fraud and obscurity.

5. Job description

A) The **Jobholders within the Policy Development and Implementation Unit** will be responsible for the following tasks:

Key responsibilities:

- Review of Union policy and law in the field of cybersecurity in the areas of electronic identities and trust services, Once Only Initiative, privacy and data protection, resilience and security of financial entities, artifical intelligence (AI) and cloud computing;

- Assist Member States and their competent authorities to develop and implement in a consistently manner Union policy and law regarding cybersecurity by means of issuing opinions, guidelines, providing and facilitating advice and best practices on topics related to current policies (e.g. NIS Directive, eIDAS, EECC, 5G, GDPR, Once Only), as well as emerging ones (e.g. NIS Directive 2.0, AI Regulation, eIDs and Digital Wallets, DORA,);
- Contribute to the work of formally established EU Expert Groups and bodies (such as the Cooperation Group, Cooperation Network) by providing its expertise and assistance; administer communities of stakeholders and international relations in the designated competence areas;
- Organise, synthetize and prioritize data information from many different sources and according to evolving or changing circumstances;
- Deal with sensitive data and information and translate these into objective and transparent policies, provide independent opinion and analysis as well as carry out preparatory work;
- Act as an expert in specific domains of cyber security and take responsibility to drive policy development and implementation from this perspective;
- Lead and be perceived as trusted advisor in Policy Management and Implementation, be up to speed with latest developments and assess their impact on policy development;
- Bring a strategic perspective on policy development by creating synergies on policy development across functional as well as geographical domains;
- Performing other duties as instructed by the management, according to the needs and priorities of ENISA.

B) The **Jobholder within the Capacity Building Unit** will be responsible for the following tasks:

Key responsibilities:

- Contribute to the development, implement and evaluatate National Cyber Security Strategies (NCSS);
- Support the development and implementation of cyber security exercises (tabletop, operational, technical);
- Contribute to the development as well as delivery (both online and physical) of cyber security trainings targetting different audiences ranging from technical (targeting CSIRT communities) to tacticals for members of national authorities and EU Institutions;
- Develop and organise Capture The Flag (CTF) competition including attack defence scenarios (read team blue team);
- 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;
- Contribute to the Agency's skills development and capacity building activities, such as the organisation and management of exercises, challenges, trainings etc.;
- Perform threat assessments and risk analysis in the area of cybersecurity, including emerging technologies;
- Performing other duties as instructed by the management, according to the needs and priorities of ENISA.

C) The **Jobholder within the Operational Cooperation Unit** will be responsible for the following tasks:

Key responsibilities:

- Contribute to the production of cyber threat intelligence (CTI) and cyber threat situational awareness for different groups of stakeholders, including both technical and non-technical audience, using available sources of information;

- Support briefing of ENISA's CTI and situational awareness deliverables to relevant stakeholders;
- Contribute to operational working practices of ENISA situational awareness mechanism and program;
- Manage CTI and situational awareness projects and resources according to ENISA Work Program;
- Contribute to existing cooperation and information sharing mechanisms (CyCLONe, CSIRTs Network etc) as needed;
- Engage in the structured cooperation with CERT-EU;
- Support the Operational Cooperation activities of the Agency;
- Performing other duties as instructed by the management, according to the needs and priorities of ENISA.

6. Qualifications and experience required[3]

6.1. Eligibility Criteria

- Be Temporary Agent 2(f) who, on the closing date for applications and on the day of filling the vacant post, are employed within their current Agency in a grade and function group corresponding to the published function group and grade bracket AD5 - AD6;
- Have at least 2 years' service within their current Agency before moving;
- Have successfully completed the probationary period provided for in Article 14 of the CEOS, in the relevant function group;
- Thorough knowledge of one of the official languages of the European Union and a satisfactory knowledge of another official European language[4].

In addition, in order to be eligible a candidate must:

- Be a national of one of the Member States of the European Union[5];
- Be entitled to his/her full rights as a citizen[6];
- Have fulfilled any obligations imposed by the applicable laws concerning military service;
- Be physically fit to perform the duties linked to the post[7].

6.2. Selection criteria

High Scoring Criteria (5 points per criterion)

- Proven experience in the tasks described in the job description, from which at least 3 years attained in the field of cybersecurity within national, international or EU context.
- Proven experience and knowledge of cybersecurity acquired in a national, international or EU environment.

[3] Candidates must meet this requirement on the closing date of application.
[4] Recruited candidates shall be required to demonstrate before their first promotion the ability to work in a third European Community language.
[5] It should be noted that due to the withdrawal of the United Kingdom from the European Union on the 31/01/2020, British nationals who do not hold the nationality of another European Union member state, are not eligible for applications at ENISA due to the fact that they do not fulfil the requirements of Article 12.2 of the Conditions of Employment of Other Servants, namely that they do not hold the nationality of an EU Member State.
[6] Prior to the appointment, the successful candidate will be asked to provide a certificate issued by a competent Member State Authority attesting the absence of any criminal record.
[7] Before appointment, the successful candidate shall be medically examined in line with the requirement of Article 28(e) of the Staff Regulations of Officials of the European Communities.

- Experience in cyber-security policy implementation and coordination activities in an international environment with a good understanding of the EU cybersecurity policy framework and the actors involved.
- Strong communication skills in English, both orally and in writing, at least at level C1[8].

Low Scoring Criteria (2 points per criterion)

- Previous experience in project management and implementation skills, and knowledge and experience in foundation information security and risk management concepts
- Experience with and/or good knowledge of modern security tools and products.
- Experience in technical reviews related to cyber security aspects, law at national or international level, and awareness raising measures.
- Experience in engaging and assisting stakeholders, preferably Member States' authorities, in cyber security policy areas mentioned under section 5 of the vacancy notice.
- Knowledge and experience with CTI practices, tools, standard CTI work practices and have the ability to work with CTI communities.
- Knowledge and experience in analysing cyber threat landscape, threat actors' techniques, tactics and procedures (TTPs).

Moreover, the following competencies will be assessed during the selection process (interview and written test):

- Excellent ability to work cooperatively with internal and external stakeholder, in multicultural teams and across organisational boundaries.
- Ability to organise and prioritise work.
- Demonstrate adaptability, flexibility and critical thinking.
- Demonstrate strong service oriented attitude.
- Ability to conduct research, to collect, analyse and report information.

IMPORTANT:
All high scoring and low scoring criteria are evaluated in order to identify the candidates to be invited for an interview and written test. The top candidates (number of the shortlisted candidates scoring above the threshold to be set by the selection board) will be invited for an interview and written test. Therefore, candidates are recommended to give evidence of their knowledge by specific examples and/or detailed professional experience in the application form in order to be evaluated in the best possible way. To that purpose candidates are requested to be as detailed and as clear as possible in the description of their professional experience and specific skills and competencies.

7. Selection procedure

The selected candidate will be appointed to a position according to the needs of the Agency, on the basis of the reserve list of candidates, proposed by the Selection Board and established following an open selection process involving interviews and written tests.

More specifically, the Selection Board decides on those candidates who are admitted to the selection procedure in accordance with the requirements as specified in the vacancy notice. The applications of

[8] Cf. Language levels of the Common European Framework of reference: http://europass.cedefop.europa.eu/en/resources/european-language-levels-cefr

the candidates admitted to the selection procedure are reviewed and the Selection Board decides on those candidates who are invited to attend an interview and written test.

The Selection Board adheres strictly to the conditions of admission laid down in the vacancy notice when deciding whether candidates are to be admitted. Candidates admitted to a previous selection procedure will not automatically be eligible. Should the Selection Board discover at any stage in the procedure that the candidate does not meet one or more of the general or special conditions for admission to the selection procedure or that the information on the application form does not correspond with the supporting documents, the candidate will be disqualified.

Shortlisted candidates will be asked to undergo a written test of which the candidates will be informed in advance. The interview and the written test are conducted in English. In case English is the mother tongue of an applicant, some interview/written test questions may be asked in the language they indicate on the application form as their second EU language.

Shortlisted candidates will be required to submit electronically relevant supporting documentation demonstrating their educational qualifications and work experience. **It is envisaged that the interviews and written test will take place in October 2021.** The date may be modified depending on the availability of the Selection Board members. Shortlisted candidates may also be required to provide work-related references upon request of the Agency. The activity of the Selection Board ends with the drawing of a reserve list of suitable applicants to occupy the position advertised. **Candidates should note that inclusion on the reserve list does not guarantee recruitment.**

The reserve list will be valid until 31/12/2022 and may be extended by decision of the Appointing Authority for a further 12 months. This list may be used to recruit Staff for other positions in the areas referred to in this vacancy.

Candidates invited to an interview will be informed by e-mail whether or not he/she has been placed on the reserve list. The appointed candidate will be asked to fill a specific form informing the Appointing Authority of any actual or potential conflict of interest[9]. If a letter of intention is issued, the candidate must undergo a compulsory medical examination to establish that he/she meets the standard of physical fitness necessary to perform the duties involved and the candidate must provide original or certified copies of all relevant documents.

In line with the European Ombudsman's recommendation, ENISA publishes the names of the Selection Board on its website once established. 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.

All enquiries or requests for information in relation to the competition, including details about candidates' results[10] should be addressed to the following email address recruitment@enisa.europa.eu

8. Conditions of Employment

ENISA and the selected Temporary Agent shall conclude a contract of employment which ensures continuation of his/her employment and career in the category of TA 2(f). That contract shall be

[9] In compliance with Article 11 of the Staff Regulations of Officials and Conditions of Employment of Other Servants of the European Union.

[10] This request for further information does not influence the timeline for lodging an appeal under Article 90 (2) of Staff Regulations of Officials and Conditions of Employment of Other Servants of the European Union.

concluded without interruption of the contract concluded with the Agency of origin ("the preceding contract") and shall fulfil the following requirements, in particular:

- The same grade and the same seniority in the grade as the preceding contract.
- The same step and the same seniority in step as the preceding contract.

The end date of the contract concluded with ENISA and of the preceding contract shall be the same. In the event that the preceding contract comes to its natural end on the day of the move, the duration of the contract concluded shall be the same as that ENISA would have set in case of a renewal of one of its own TA 2(f).

The selected Temporary Agent shall take up duty at ENISA up to three months' after the job offer, unless it is otherwise agreed between the two Agencies and the Staff Member concerned.

The Agency of origin shall transfer the personnel file to ENISA no later than 30 days after the date of the move.

The rights and entitlements inherent to the country of employment (i.e. Greece) will be adapted accordingly.

9. 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 selections.

10.Equal opportunity

ENISA is an equal opportunities employer and accepts applications without distinction on the grounds of sex, racial or ethnic origin, religion or belief, age or sexual orientation, marital status or family situation. Applications from women and disabled candidates are encouraged. If you have a disability or medical condition that may hinder ability to sit the interview or written test, please indicate this in your application and let us know the type of special arrangements you need. The staff is recruited on the broadest possible geographical basis from among nationals of all Member States of the European Union.

11.Complaints

If a candidate considers that he or she has been adversely affected by a particular decision, he or she can lodge a complaint under Article 90(2) of the Staff Regulations of Officials and Conditions of Employment of Other Servants of the European Union, within 3 months from the date of notification to the following address:

Executive Director
European Union Agency for Cybersecurity (ENISA)
Ethnikis Antistaseos 72 & Agamemnonos St. Chalandri
15231, Attiki
Athens, Greece

Should the complaint be rejected, pursuant to Article 270 of the Treaty of the Functioning of the European Union and Article 91 of the Staff Regulations of Officials and Conditions of Employment of

Other Servants of the European Union, a candidate may request judicial review of the act. The appeal must be lodged within 3 months from the date of notification, to the following address:

Registry
The General Court
Rue du Fort Niedergrünewald
L-2925 Luxembourg
Luxembourg

Please note that the Appointing Authority does not have the power to amend the decisions of a Selection Board. The General Court has consistently held that the wide discretion enjoyed by Selection Boards is not subject to review by The General Court unless rules which govern the proceedings of Selection Boards have been infringed. For details of how to submit an appeal, please consult the website of the Court of Justice of the European Union: http://curia.europa.eu

It is also possible to complain to the European Ombudsman pursuant to Article 228 of the Treaty on the Functioning of the European Union as well as the Statute of the Ombudsman and the implementing Provisions adopted by the Ombudsman under Article 14 of the Statute.

European Ombudsman
1 Avenue du President Robert Schuman
CS 30403
67001 Strasbourg Cedex
France
http://www.ombudsman.europa.eu

Please note that complaints made to the Ombudsman have no suspensive effect on the period laid down in Articles 90 (2) and 91 of the Staff Regulations for lodging complaints or for submitting appeals to the General Court pursuant to Article 270 of the Treaty of the Functioning of the European Union. Please note also that under Article 2(4) of the General conditions governing the performance of the Ombudsman's duties, any complaint lodged with the Ombudsman must be preceded by the appropriate administrative approaches to the institutions and bodies concerned.

12. Submission of applications

For an application to be valid candidates **shall:**

- Use the PDF application form related to the position you want to apply. The form is available on ENISA career website. The format of the PDF application must not be changed and filled accordingly to the instructions. The application must be submitted in English language, which is the working language of ENISA.
- Send your application within the set deadline by e-mail to: inter-agency-mobility@enisa.europa.eu
- Indicate in the subject of the e-mail: **FAMILY NAME-FIRST NAME-2021-05-IAM**

Incomplete applications will be disqualified and treated as non-eligible. Candidates should submit a separate application for each vacancy they want to apply for.

At this stage of the selection procedure candidates are not required to send any additional supporting documents with the application (i.e.: copies of your ID-card, educational certificates, evidence of previous professional experience etc.). **Candidates are reminded not to wait until the final days before the closing date for applications.**

Please note that the selection process may take several months. Status of the selection procedures can be consulted at: https://www.enisa.europa.eu/recruitment/vacancies/status-of-recruitment-procedures

The **closing date** and time for the submission of applications is:

30/08/2021 (16h00 CET)

Published on ENISA website: 28/07/2021