

Vacancy Notice

Cybersecurity Officer (CA FGIV) – Two positions

Ref. ENISA-CA-FGIV-2021-04

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 **two cybersecurity officers** will be recruited, 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 8: Market, cybersecurity certification and standardisation

Please send us your applications by no later than 06/09/2021 at 16:00 CET¹.

1. The Agency

The European Union Agency for Cybersecurity (ENISA) holds a discreet and enhanced role under the mandate of the Cybersecurity Act Regulation². 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 **Athens, Greece**.

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/>

¹ Initial deadline for applications was 23.08.2021 at 16:00 CET. The deadline for submission of applications is extended till 06.09.2021 at 16:00 CET.

² Regulation (EU) 2019/881 - Cybersecurity Act: <http://data.europa.eu/eli/reg/2019/881/oj>

2. Policy Development and Implementation Unit

The Cybersecurity Officer will work in the Policy Development and Implementation Unit (PDI).

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. Market, Certification and Standardisation Unit

The Cybersecurity Officer will work in the Market, Certification and Standardisation Unit (MCS).

The Market, Certification and Standardisation unit ensures the performance of the tasks of the Agency as set out in Art.8 and 22 and under Title III of the CSA, pursuant Article 2(5) of the MB Decision MB/2020/9. It is responsible and leads the activities relevant to achieving the strategic objective “High level of trust in secure digital solutions”. The Unit contributes in achieving the overall goals of the Agency as described through the recitals 4, 11-13, 23, 42, 44-45, 48, 50-53 of the CSA.

The unit undertakes efforts to increase the security of ICT products, ICT services and ICT processes and thus increase citizens’, organizations’ and businesses’ trust in digital solutions. For this, the unit develops and maintains certification schemes, works with organizations, manufacturers or providers involved in the design and development of ICT products, ICT services or ICT processes and products. It promotes the implementation of ‘security by design’ and ‘security by default’ measures and other approaches to reduce the risk of harm from malicious exploitation and protecting the security of ICT products, services and processes to the highest possible degree throughout their lifetime. The work of the Unit in increasing the security of ICT products, ICT services and ICT processes contributes to efficient and effective implementation of the Union’s legal framework on protecting consumer’s data and privacy. MCS contributes to the development of the cybersecurity industry in the Union, in

particular SMEs and start-ups, to reduce dependence on cybersecurity products and services from outside the Union and to reinforce supply chains inside the Union.

The unit develops relations and consults regularly standardisation organisations, in particular European standardisation organisations. It liaises with the relevant organisations that represents the interests of consumers, European Data Protection Board and other authorities that deal with data protection, as well as with other relevant bodies at national and Union level and with public and private stakeholders dealing with ICT products, services and processes.

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.

4. Job description

The **Jobholders** will be responsible for the following tasks:

Key responsibilities pertaining to Policy Development and Implementation Unit (PDI):

- Assist in reviewing Union policy and law on current policy areas of the Agency (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 ENISA's efforts in building up a framework for supporting evidence based policy making in the policy areas mentioned above.
- Contribute to a team that assists Member States and their competent authorities to develop and implement Union policy and law in a consistently, transparent and effective manner.
- Contribute to a team that supports 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.

- Contribute to ENISA's efforts in organising, synthesizing and prioritizing sensitive information from many different sources and translate them into objective, consistent and transparent policy options and analysis.
- Contribute to a team that would develop a strategic perspective on policy development and implementation across different policy areas, sectors, and technologies.
- Performing other duties as instructed by the management, according to the needs and priorities of ENISA.

Key responsibilities pertaining to Market, Certification and Standardisation Unit (MCS):

- Assist to the design, deployment and maintenance of EU cybersecurity certification schemes and the EU cybersecurity certification framework.
- Support with compiling and publishing guidelines and develop good practices, concerning the cybersecurity requirements for ICT products, ICT services and ICT processes, in cooperation with national cybersecurity certification authorities and industry in a formal, structured and transparent way.
- Assist in the area of cybersecurity market as a horizontal area of interest focusing on market segments, supply and demand etc. ENISA produces reports, analyses and recommendations thereto.
- Assist to 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.
- Assist in the promulgation of draft candidate cybersecurity certification schemes by analysing requirements for security measures and controls in the relevant policy areas including, cloud services, common criteria, Trust services, personal data and privacy, internet of things, artificial intelligence, risk management and assessment etc. in line with the Union Rolling Work Program and certification requests.
- Assist to the drafting and implementation of the Agency Multiannual Work Programme.
- Assist to tender procedures and supervision of contracts related to the activities of the Multiannual Work Programme.
- Assist in setting-up and co-ordinating expert/working groups in the area of cybersecurity.
- Assist European Union institutions, bodies, offices and agencies and the Member States on research needs and priorities in the field of cybersecurity.
- Performing other duties as instructed by the management, according to the needs and priorities of ENISA.

5. Qualifications and experience required³

5.1. Eligibility Criteria

- A level of education which corresponds to completed university studies of at least three years attested by a diploma⁴.

³ Candidates must meet this requirement on the closing date of application.

⁴ Only diplomas issued by EU Member State authorities and diplomas recognised as equivalent by the relevant EU Member State bodies are accepted. If the main studies took place outside the European Union, the candidate's qualification must have been recognised by a body delegated officially for the purpose by one of the European Union Member States (such as a national Ministry of Education) and a document attesting so must be submitted if you have been invited for an interview. This will enable the selection board to assess accurately the level of the qualifications. Candidates must meet this requirement on the closing date of application.

- Have a thorough knowledge of one of the official languages of the European Union and a satisfactory knowledge of another official European language⁵.
- Be a national of one of the Member States of the European Union⁶.
- Be entitled to his/her full rights as a citizen⁷.
- Have fulfilled any obligations imposed by the applicable laws concerning military service.
- Be physically fit to perform the duties linked to the post⁸.

5.2 Inter-Agency and Internal Mobility

Contract Agents, Function Group IV from EU Agencies are also invited to apply in accordance with the following ENISA rules: **Decision No MB/2019/14 of the Management Board of the European Union Agency for Network and Information Security (ENISA) adopting Implementing rules on the general provisions for implementing Article 79(2) of the Conditions of Employment of Other Servants of the European Union, governing the conditions of employment of contract staff employed under the terms of Article 3a.**

5.3 Selection criteria

High Scoring Criteria (5 points per criterion)

- Proven experience in the tasks listed under the job description, pertaining to one of the indicated units (i.e. PDI or MCS), 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.
- Experience in cybersecurity policy implementation and coordination activities in an national, international or EU environment.
- Experience in managing technical reviews related to cybersecurity aspects.
- 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 C1⁹.

⁵ Please note that the minimum levels required above must apply to each linguistic ability (speaking, writing, reading and listening). You must have knowledge of at least two official EU languages: language 1 at minimum C1 level (thorough knowledge) and language 2 at minimum B2 level (satisfactory knowledge). These abilities reflect the Common European Framework of Reference for Languages <https://europass.cedefop.europa.eu/resources/european-language-levels-cefr>. The official languages of the European Union are: Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, and Swedish.

⁶ 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.

⁷ 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.

⁸ 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.

⁹ Cf. Language levels of the Common European Framework of reference: <http://europass.cedefop.europa.eu/en/resources/european-language-levels-cefr>

Low Scoring Criteria (2 points per criterion)

- Previous experience in project management and implementation skills.
- Proven knowledge (acquired through training or experience) of area(s) covering the operational mandate of ENISA as defined in the Cybersecurity Act.
- Experience in assisting in the engagement of stakeholders, preferably in cybersecurity policy areas mentioned under section 4 of the vacancy notice.

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

- Ability to work cooperatively with internal and external stakeholder, in multicultural teams and across organisational boundaries.
- Ability to organise and prioritise work.
- Demonstrate focus on excellence and quality.
- Ability 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 competences.

6. 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 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 September/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. The reserve list is unranked and is drawn alphabetically. **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 candidates will be asked to fill a specific form informing the Appointing Authority of any actual or potential conflict of interest¹⁰. 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' results¹¹ should be addressed to the following email address recruitment@enisa.europa.eu

7. Conditions of Employment

The successful candidate (s) will be recruited as member of the contractual staff, pursuant to Article 3a) of the Conditions of Employment of Other Servants of the European Union, for a period of three (3) years. This contract may be renewed for a period of five (5) years with the possibility of an indefinite contract at the end of the renewal of five (5) years. The appointment will be in Function Group IV. Successful candidates who are offered a contract of employment will be graded on entry into service in step 1 of the relevant grade 13, 14 or 16. The grade will be determined in accordance with the number of years of professional experience of the successful candidate.

In addition, successful candidates, who are recruited shall undergo an initial probation period of 9 months. Due to the Agency's operational requirements, the successful candidate will be required to be available at the shortest possible notice.

The remuneration of staff members consists of a basic salary¹² and where applicable allowances.

¹⁰ In compliance with Article 11 of the Staff Regulations of Officials and Conditions of Employment of Other Servants of the European Union.

¹¹ 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.

¹² Basic Salary: there is a basic salary scale for each grade, divided into a number of steps. The final step is defined according to the total number of years of experience starting from the education certificate/degree giving access to the position.

This salary will be weighted by the corrective coefficient applicable to the hosting country of the agency. The current corrective coefficient is 81.4 %, which will be reviewed yearly, in the end of the year, with retroactive effect from 1 July.

The staff member depending on its personal situation may be entitled to various allowances, in particular to an expatriation (16 % of basic gross salary) or to a foreign residence allowance (4 % of basic gross salary) and to family allowances (depending on personal situation) such as household allowance, dependent child allowance, pre-school allowance. In addition, the successful candidate might be entitled to temporary daily allowance¹³, installation allowance¹⁴ etc.

Tabel 1 – Example of net monthly salary¹⁵

FGIV Grade 13 (less than 5 years of work experience after the relevant diploma)		
a) Minimum final net salary (without any allowances)	b) Final net salary with expatriation allowance	c) Final net salary with expatriation, household and 1 dependent child allowance
2,442.48 €	2,817.92 €	3,526.98 €
FGIV Grade 14 (between 5 years and 17 years of experience after the relevant diploma)		
a) Minimum final net salary (without any allowances)	b) Final net salary with expatriation allowance	c) Final net salary with expatriation, household and 1 dependent child allowance
2,640.88 €	3,164.89 €	3,891.24 €
FGIV Grade 16 (more than 17 years of work experience after the relevant diploma)		
a) Minimum final net salary (without any allowances)	b) Final net salary with expatriation allowance	c) Final net salary with expatriation, household and 1 dependent child allowance
3,299.16 €	3,969.98 €	4,744.74 €

Other benefits include:

- Special ID card, issued by the Greek Ministry of Foreign Affairs.
- Special car license plates (for certain grades).
- Education allowance.
- Home visit allowance.

¹³ If staff member is requested to change the residence in order to take up duties, she/he will be entitled to: reimbursement of the travel costs; temporary daily subsistence allowance (43.97 EUR for up to 10 months or 35,46 EUR for 120 days, if no dependents).

¹⁴ The installation allowance is granted (depending on the personal situation) for 1 or 2 months of the basic salary and is paid upon successful completion of the nine months probationary period.

¹⁵ The current corrective coefficient is 81.4 %, which will be reviewed yearly, in the end of the year, with retroactive effect from 1 July.

- Additional financial support for the education of children “subject to budget availability and conditions”.
- VAT exemption allowance on certain goods for a period of 3 years.
- Importation/purchase of 1 or more vehicles depending on the circumstances without taxes of VAT (“special conditions apply”).
- Staff is entitled to annual leave of two working days per each complete calendar month of service , plus additional days for the grade, age, home leave for expatriates and an average of 19 public holidays pe year.
- In addition, staff may be granted special leave for certain circumstances such as marriage, borth, adoption of a child, moving, elections, serious sickness of spouse etc.
- ENISA staff members benefit of health isurance 24/7 and world wide by the Joint Insurance Scheme (JSIS).
- Statutory staff who have completed at least 10 years of service or reached pensionable age, are entitled to a pension under the pension scheme of the European Union institutions (PSEUI).
- Where it is considered in the interest of the service, statutory staff may avail of the ENISA teleworking policy and flexible working time arrangements.
- A wide range of learning and professional development opportunities.

It should be noted that a Seat Agreement between ENISA and the Hellenic Authorities further gives privileges for the employees of the Agency which are not fully listed above.

Further information on working conditions of Temporary staff and Contract staff can be found in the [Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union](#).

8. Community Tax

The salaries of staff members are subject to a Community tax deducted at source. They are exempt from national tax on salary and are members of the Community social security and pension schemes.

For additional information about salaries, deductions and allowances please consult the [Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union](#).

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.
- Indicate in the subject: **FAMILY NAME-FIRST NAME-2021-04**

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:

06/09/2021 (16h00 CET)

Published on ENISA website: 20/07/2021