Vacancy Notice for the position of ICT Officer / Local Information Security Officer (CA FGIV)

Publication:
External: Contractual Agent Function Group IV
For Inter-agency applicants: Contractual Agent Function Group IV.

Title of Function: ICT Officer / Local Information Security Officer
Number of persons to be selected for the reserve list: up to 4
Number of persons to be recruited: up to 1

Reference: **ECCC/CA/2023/10/ITO**

Contents

1. Introduction

We are

The European Cybersecurity Industrial, Technology and Research Competence Centre (hereafter "ECCC") was established by Regulation (EU) 2021/ 887[1]. In accordance with the article 3 of that Regulation, the mission of the Centre, and the related Network of National Coordination Centres, is to:

- Strengthen leadership and strategic autonomy of the European Union ("EU" or "the Union") in the area of cybersecurity by retaining and developing the EU's research, academic, societal, technological and industrial cybersecurity capacities and capabilities necessary to enhance trust and security in the Digital Single Market, including by retaining and developing the confidentiality, integrity and accessibility of data.
- Support EU technological capacities, capabilities and skills in relation to the resilience and reliability of the infrastructure of network and information systems, including critical infrastructure and commonly used hardware and software in the Union.
- Increase the global competitiveness of the Union's cybersecurity industry, ensure high cybersecurity standards throughout the Union and turn cybersecurity into a competitive advantage for other Union industries.
- Undertake these tasks in collaboration with the European Union Agency for Cybersecurity (ENISA) and the Cybersecurity Competence Community, as appropriate.
- In accordance with the legislative acts establishing the relevant programmes, in particular Horizon Europe and the Digital Europe Programme, use relevant Union financial resources in such a way as to contribute to the mission mentioned above.

This mission is translated into objectives and tasks of the ECCC, which are specified respectively in articles 4 and 5 of the referred Regulation.

The ECCC will be made up of 37 staff initially and will manage a budget of about EUR 200 million per year.[2]

The ECCC will be located in Bucharest, English will be the language commonly used to exercise its tasks.

For further information, please consult the following website: European Cybersecurity Competence Centre and Network (europa.eu)

[1] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (europa.eu) OJ L 202, 8.6.2021, p. 1–31

[2] Staff and budget numbers based on projections for 2023.

2. Job description

The ICT Officer / Local Information Security Officer will be performing a wide range of tasks related to operational IT Management, IT system management, IT support, Logistic support, documents and record management, and local information security.

Duties and responsibilities

More specifically, as a member of the ECCC, under the supervision of the Executive Director:

Operational IT Management

- To contribute to develop and ensure the correct operation of the systems;
- To run technical, functional and integration testing and carrying out capacity analysis and system evaluation;
- To apply security procedures;
- To apply IT quality plans defined by the ECCC;
- To contribute to improvement and maintenance of IT tools, products, projects, services through technical watch;
- To represent the ECCC in internal and external meetings in relation with the ICT domain or call and projects management.

IT System Management:

- Contribute to develop and implement of the ICT strategy and planning;
- To provide expertise on the integration of information systems into the ECCC;
- Design, installation and configuration of servers in a virtual environment (EC2 instance or Azure VM)
- Management and monitoring of cloud native storage SAN, NAS, and or S3 type of technologies (Ceph/Amazon EBS or Azure managed Disk).
- Development of scripts to automate system management tasks. (Ansible, Teraform, Cloudformation, Azure Automation State Configuration)
- Monitoring of servers, incident resolution, preliminary diagnosis of software and hardware problems
- Architecture, design and configuration of server software and systems components
- Ensure the capacity management, contingency planning, IT service continuity management, automation of repetitive tasks, and implementation of security recommendations.
- To contribute to correct operation of the systems and application of the procedures;

IT Support: IT Support in service management

- To install new applications on the servers including acceptance tests;
- To define, prepare, distribute and support IT reference solutions;
- To provide first and second level support;
- To produce technical, management and user oriented documentation.

Logistic support / dispatching

- To monitor the location of equipment, good and /or work crews in order to coordinate service and schedules;
- To record and maintain files and records of requests, work, or service performed, inventories and / or other dispatch information;
- To ensure relations with services in order to address questions, problems and / or requests relating to equipment, goods and / or work crews.

Documents and record management

- Until the recruitment/appointment of a dedicated Document Management Officer, at a later stage: To define the needs, advice and provide solutions to management in the area of workflow management tools concerning the ECCC's processes;
- To ensure the maintenance of the ECCC's IT-tools for workflow management;
- To ensure access to the documents (both paper and electronic) concerning the activities of the unit, taking account of the relevant provisions on security and data protection;
- To carry out tasks related to the physical protection, conservation and transfer of documents records and files (both paper and electronic).

Local Information Security Officer tasks

- Developing and managing the ECCC security plans, processes and policies to attain compliance to European Commission Security legislation for what concerns ICT systems
- Contributing to the dissemination of the information systems security policy by proposing awareness-raising and annual mandatory training programmes for staff and contractors
- Collaborating with the ECCC Local Security Officer and acting as IT security adviser
- Collaborating with the ECCC Data Protection Officer (DPO) and supporting the implementation of the ICT processes related to the data protection
- Overseeing the development of the security plans
- Organising the IT security audits and reviews in all ECCC site
- Performing other duties relevant to the role of LISO when identified by management or as required by legislation

Other tasks

- Contribute to other relevant tasks related to the setting up of the ECCC in Bucharest.

Some travel to Brussels and other locations in the EU may be required.

3. Eligibility and selection criteria

Eligibility criteria

In order to be eligible, candidates must fulfill by the closing date for applications and maintained throughout the selection procedure and appointment the following criteria:

- Have a level of education which corresponds to completed university studies of at least 3 years attested by a diploma[3] and, after having obtained the diploma, at least 5 years full-time of appropriate professional experience;
- Be a national of a Member State of the European Union and enjoy full rights as a citizen;
- Have fulfilled any obligations imposed by the applicable laws concerning military service.
- Produce the appropriate character references as to their suitability for the performance of duties of the post[4].
- Have a thorough knowledge of one of the official EU languages and a satisfactory knowledge (at least at the B2 level or equivalent) of another of these languages to the extent necessary for the performance of their duties (candidates are invited to specify in their CV possible language certificates they have obtained and which can demonstrate their language skills).
- Be physically fit to perform the duties linked to the post. Before being engaged, a member of the temporary staff shall be medically examined by one of the institution's medical officers in line with the requirement of Art. 12(2) (d) of the Conditions of Employment of Other Servants (CEOS)[5].

[3] Only qualifications issued by EU Member State authorities and qualifications recognised as equivalent by the relevant EU Member State authorities will be accepted.

[4] Prior to the appointment, the successful candidate will be asked to provide a certificate issued by the competent authority attesting the absence of any criminal record.

[5] Conditions of Employment of Other Servants (CEOS) of the European Union, which is available on the following web page: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1962R0031:20140101:EN:PDF

Selection criteria

Candidates selected on the basis of the above eligibility criteria will then be evaluated according to the following selection criteria:

Essential

- A University degree on Information and Technology, Engineering/Science, Computer Science, Cybersecurity or any other domain that is deemed relevant to the post;
- Minimum 5 years of professional experience with tasks closely related to those described in section '2. Job Description – Duties and responsibilities';
- Professional experience with security aspects of ICT systems, preferably for processing of classified information;
- Excellent written and oral communication skills, with demonstrated ability to communicate administrative, financial and business information at all levels inside and outside the organization;
- Excellent command of written and spoken English

Advantageous

- Working experience in a field related to the duties in an international and multicultural environment, preferably within a European Institution or body.
- Practical experience/knowledge of European Commission IT systems and procedures

In order to be evaluated in the best possible way, candidates are recommended to give evidence of their knowledge with specific examples and/or detailed professional experience. Candidates are invited to be as detailed and as clear as possible in the description of their professional experience and specific skills and competences in their application form.

Failure to comply with eligibility or essential selection criteria will result in a disqualification of the applicant concerned.

In addition, the ECCC is looking for candidates with the following competencies:

- Critical thinking, analysing and creative problem-solving
- Decision-making & getting results
- Information management (digital and data literacy)
- Self-management
- Working together
- Learning as a skill

- Communication
- Intrapreneurship

4. Independence and declaration of interest

The successful candidate will be required to make a declaration of commitment to act independently in the public interest and to make a declaration in relation to interests, which might be considered prejudicial to her/his independence. Candidates must confirm their willingness to do so in their application.

5. Selection and appointment procedure

Selection and assessment of the application

For each selection process, a Selection Committee is nominated by the Executive Director of the ECCC.

After applications are screened, the Selection Committee, having regard to the vacancy notice and basing itself on elements of the application, will draw up a list of suitable candidates to be invited for an interview and a written test, which will both be held in Brussels, or remotely. The candidates not invited to the interview and the written test will be informed that they were not selected.

The interview and written test will assess the candidate's suitability with regard to the selection criteria mentioned above.

The Selection Committee may also decide to include additional tests.

Reserve list

On the basis of the above procedure, the Selection Committee will establish a reserve list.

Invitation to the interviews with the Executive Director

The applicants on the reserve list may be invited to an interview with the Executive Director.

Appointment

The recruitment will take place upon a decision of the authority authorised to conclude contracts of employment of the ECCC.

The Executive Director will select successful candidates from the reserve list and offer them a

post. A binding commitment can only be made after the verification of all conditions[6] and will take the form of a contract signed by the Executive Director.

The reserve list could be used to fill other positions within the ECCC for the same profile. The reserve list will be valid until 31 December 2024 and may be extended at the discretion of the Appointing Authority. Candidates should note that inclusion on the reserve list does not guarantee recruitment. Recruitment will be based on availability of posts and budget.

The ECCC may decide at any time of the procedure not to pursue the recruitment.

6. Equal opportunities

The ECCC, as a Union body, applies a policy of equal opportunities and non-discrimination in accordance with Article 1d of the Staff Regulations[7].

7. Conditions of employment

The successful candidate will be appointed by the Appointing Authority of the ECCC as contractual agent pursuant to Article 2(f) of the Conditions of Employment of Other Servants of the European Union, for an initial period of 2 years, which may be renewed.

For all applicants, the grade offered is Contractual Agent function group IV.

For Interagency applicants, the grade offered is Contractual Agent function group IV.

To be eligible for interagency mobility, you must satisfy all of the following requirements on the closing date for submission of applications and on the day of filling the vacant post:

- be employed in one of the EU agencies in function group IV ;
- have served for at least three years as contract staff within your current agency;
- have successfully completed the probationary period provided for in Art. 14 of the CEOS in the relevant function group.

A probation period of 9 months will apply for external applicants but not for applicants eligible for interagency mobility.

In addition to their basic salary, staff members may be entitled to various allowances in particular an expatriation or foreign residence allowance, family allowances including household allowance, dependent child allowance, pre-school allowance and an education allowance.

For any further information on contractual and working conditions, please refer to the Staff

[6] Before the appointment, a successful candidate shall undergo a medical examination by the medical services of the Commission in order that the ECCC may be satisfied that she/he fulfils the requirement of article 28(e) of the Staff Regulation of the Officials of the European Union.

[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1962R0031:20140101:EN:PDF

Regulations of Officials and the Conditions of Employment of Other Servants (CEOS) of the European Union, which is available on the following web page:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1962R0031:20140101:EN:PDF

The place of employment is Bucharest, where the ECCC premises are located.

English is the language that is commonly used in the exercise of the tasks.

8. Application procedure

Applications must only be sent by e-mail to the mailbox CNECT-ECCC-VACANCIES@ec.europa.eu quoting the reference.

Applications must include:

1. Application form (ANNEX II – APPLICATION FORM of this vacancy note)
2. Curriculum Vitae (CV) in the European CV format[8]

All documents mentioned above must be submitted and should be named starting with the family name of the candidate.

Supporting documents (e.g. certified copies of degrees/diplomas, references, proof of experience, etc.) should not be sent at this point but must be submitted at a later stage of the procedure if requested. The ECCC has the right to disqualify applicants who fail to submit all the required documents.

In order to facilitate the selection process, application documents as well as all communications to candidates concerning this vacancy will be **in English only**.

The application will be rejected if the dossier is incomplete.

Candidates are advised to apply using an e-mail address that will remain valid for several months: candidates that will leave their job in the coming months are advised not to use their professional e-mail address.

When filling in their application, candidates are requested to provide examples of their professional experiences and competences.

Candidates are asked to report any potential change of contact details without delay, to the following e-mail address: CNECT-ECCC-VACANCIES@ec.europa.eu . Please remember to quote

[8] http://europass.cedefop.europa.eu/en/documents/curriculum-vitae/templates-instructions

the reference of the vacancy for which you have applied in all correspondence: **ECCC/CA/2023/10/ITO.**

Candidates are reminded that the Selection Committee's work is confidential. It is forbidden for candidates to make direct or indirect contact with the Selection Committee members or to ask anybody else to do so, on their behalf.

For each position, any new application made by a candidate with the same e-mail address will automatically erase and replace the previous application for that position.

Closing date Applications must be completed and submitted by **Wednesday, 21st of June 2023, 23:59 CET** (Central European Summer Time / Brussels time).

9. Applicants' privacy policy in the context of selection and recruitment

The personal information that ECCC requests from applicants will be processed in line with Regulation (EU) 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

For more explanations on data protection, please see the annexed privacy statement.

10. Appeals

Candidates who consider that their interests have been prejudiced by any decision related to the selection procedure can take the following actions:

Request for review of the decision taken by the Selection Committee

A candidate who feels that she/he has been treated incorrectly may ask to have her/his application reconsidered by sending, within 10 calendar days of the date of notification, a request for review via e-mail to: CNECT-ECCC-VACANCIES@ec.europa.eu. The candidate should quote the number of the selection procedure concerned and address the request to the Chairman of the Selection Committee.

The Selection Committee will reconsider the application and notify the candidate of its decision within 45 calendar days of receipt of the request.

Appeals

If a candidate considers that she/he has been adversely affected by a decision of the Selection Committee, she/he can lodge a complaint under article 90(2) of the Staff Regulations within the time limits provided for at the following address:

Miguel Gonzalez-Sancho

Interim Executive Director, European Cybersecurity Competence Centre

Head of Unit, Cybersecurity Technology and Capacity Building

Directorate-General for Communications Networks, Content and Technology

Rue de la Loi 200

1049 Brussels, Belgium

The complaint must be lodged within three months. The time limit for initiating this type of procedure starts to run from the time the ECCC informs the candidate by e-mail[9].

Complaint to the European Ombudsman

It is also possible to lodge a complaint with the European Ombudsman pursuant to Article 228(1) of the Treaty on the Functioning of the European Union and in accordance with the statute of the Ombudsman and the implementing provisions adopted by the Ombudsman.

Complaints made to the Ombudsman have no suspense effect on the period laid down in the Article 91 of the Staff Regulations. 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.

[9] See the Staff Regulations as modified by Council Regulation No 723/2004 of 22 March 2004 published in the Official Journal of the European Union L 124 of 27 April 2004 – http://europa.eu/eur-lex

ANNEX I – PROTECTION OF YOUR PERSONAL DATA

WHICH OF YOUR PERSONAL DATA DO WE PROCESS?

1.1. When you apply for a job (selection process), we process:

- Identity information you provide us with, such as your first name, last name, birthdate, preferences and interests;
- Contact details you provide us with, such as your e-mail address, postal address, country and (mobile) telephone number;
- Resume information you provide us with, such as your employer, professional experience, education, skills and references;
- Results of the selection process
- Any other personal data you provide us with to support your job application or to allow the verification of the eligibility and selection criteria laid down in the vacancy notice.

1.2. For the recruitment process, we process:

- All the information from the selection process mentioned above;
- Documents verifying nationality;
- Family situation;
- Documents verifying appropriate character references (in accordance with Article 12(2) and 82(3) of CEOS);
- Document sent from the Commission Medical Service indicating that the selected candidate is physically fit or not to perform the job;
- PMO forms to allow the establishment of the recruited staff's entitlements under the Staff Regulation and CEOS;
- Originals of the extracts of criminal record/attestation of good behavior;
- Any other personal data you provide us with.

1.3. We receive most of your personal data directly from you, but it may happen that our HR department includes additional information in your job application or that we receive information from a recruitment agency. In such case, the agency is responsible to provide you with the information in this Applicants' Privacy Policy. Also, we advise you to consult the privacy policy of the recruitment agency.

1.4. We do not intend to process sensitive personal data about you, such as information revealing your racial or ethnic origin, political opinions, religious and philosophical

beliefs, trade union membership, genetic data, biometric data for the purpose of unique identification, data concerning health, sex life or sexual orientation. If such information is necessary for your job application, we will ask for your consent separately. If you nevertheless provide us with such information on your own initiative, we will derive your explicit, freely given, specific, informed and unambiguous consent to the processing of this data. Personal data concerning health (medical data) are processed by the Medical Service of the European Commission. Candidates failing to provide compulsory data as requested in the vacancy notice will be excluded from the selection process.

FOR WHAT PURPOSES DO WE PROCESS YOUR PERSONAL DATA AND WHAT IS THE LEGAL BASIS FOR THIS?

1.5. We process your personal data for selection and recruitment purposes so that you are able to apply for a job with us at this moment or in the near future, as well as to keep track of your details in this context and to follow up on your application. We rely on your consent for this processing activity. We also rely on Article 2(a) and (f), 3(a), 12, 82 and 86 of CEOS. If special categories of personal data are processed, we may rely on the derogation explicit consent (Art. 10(2)(a) of Regulation (EU) 2018/1725) or Article 137(3) of the Financial Regulation (for criminal records).

TO WHOM DO WE SEND YOUR PERSONAL DATA?

1.6. We may share your personal data with third parties in order to process your personal data for the purposes outlined above. Third parties are only allowed to process your personal data on our behalf and upon our explicit written instruction. We also warrant that all those third parties are selected with due care and are committed to observing the safety and integrity of your personal data.

1.7. We may be legally obliged to share your personal data with competent law enforcement agents or representatives, judicial authorities, governmental agencies or bodies.

1.8. We do not send your personal data in an identifiable manner to any other third party than the ones mentioned without your explicit consent to do so. However, we may send anonymised data to other organisations that may use those data for improving our job application process.

WHERE DO WE PROCESS YOUR PERSONAL DATA?

1.9. We process your personal data within the European Economic Area (EEA).

WHAT QUALITY ASSURANCES DO WE COMPLY WITH?

1.10. We do our utmost best to process only those personal data which are necessary to achieve the purposes above.

1.11. Your personal data are only processed for as long as needed to achieve the purposes listed above or up until such time where you withdraw your consent for processing them. If you are recruited, your personal data are kept for 10 years after termination of employment. If you are not recruited, your personal data are kept for 5 years after expiry of the reserve list. If you are not on a reserve list, your personal data are kept

for 5 years after the notification of non-selection.

1.12. We will take appropriate technical and organisational measures to keep your personal data safe from unauthorised access or theft as well as accidental loss tampering or destruction. Access by our personnel or third parties' personnel will only be on a need- to-know basis and be subject to confidentiality obligations. You understand, however, that safety and security are best efforts obligations which can never be guaranteed.

1.13. In compliance with Article 46 of Regulation (EU) 2021/887 of the European Parliament and of the Council, of 20 May 2021, establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres and until the ECCC is fully established and the transition period is over, the ECCC will use the data protection record adopted by the European Commission. During this period, the ECCC will also use the services of the Data Protection Officer of the European Commission.

WHAT ARE YOUR RIGHTS?

1.14. You have the right to request access to all personal data processed by us pertaining to you.

1.15. You have the right to rectification, *i.e.* to ask that any personal data pertaining to you that are inaccurate, are corrected.

1.16. You have the right to withdraw your earlier given consent for processing of your personal data.

1.17. You have the right to erasure, *i.e.* to request that personal data pertaining to you be deleted if these data are no longer required in the light of the purposes outlined in Article 3 above or if you withdraw your consent for processing them.

1.18. You have the right to restriction instead of deletion, *i.e.* to request that we limit the processing of your personal data.

1.19. You have the right to object to the processing of personal data if the processing by us is necessary for the performance of a task carried out in the public interest, unless if we demonstrate compelling legitimate grounds which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

1.20. You have the right to data portability, *i.e.* to receive from us in a structured, commonly-used and machine-readable format all personal data you have provided to us if the processing is based on your consent or a contract with you and the processing is carried out by automated means.

1.21. If you wish to submit a request to exercise one or more of the rights listed above, you can contact us by sending an e-mail to CNECT-ECCC-VACANCIES@ec.europa.eu. An e-mail requesting to exercise a right will not be construed as consent with the processing of your personal data beyond what is required for handling your request. Such request should meet the following conditions:

- State clearly which right you wish to exercise; and
- Your request should be accompanied by a digitally scanned copy of your valid identity card proving your identity.

We will promptly inform you of having received your request. If the request meets the conditions above and proves valid, we will honour it as soon as reasonably possible and at the latest thirty (30) days after having received your request.

If you have any complaints regarding the processing of your personal data by us, you may always contact us by sending an e-mail to CNECT-ECCC-VACANCIES@ec.europa.eu. If you remain unsatisfied with our response, you are free to file a complaint with the European Data Protection Supervisor (https://edps.europa.eu).

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Publication: External CA FGIV

Title of Function: ICT Officer / Local Information Security Officer

Reference: **ECCC/CA/2023/10/ITO**

ANNEX II – APPLICATION FORM

ECCC/CA/2023/10/ITO

Name and First Name:	
Nationality:	
Gender:	
Date of birth:	

Please specify:

ELIGIBILITY CRITERIA		
Have a level of education which corresponds to completed university studies of at least 3 years attested by a diploma and, after having obtained the diploma, at least 5 years full-time of appropriate professional experience.	YES ☐	NO ☐
Be a national of a Member State of the European Union.	YES ☐	NO ☐
Enjoy full rights as a citizen.	YES ☐	NO ☐
Have fulfilled any obligations imposed by the applicable laws concerning military service.	YES ☐	NO ☐
Produce the appropriate character references as to their suitability for the performance of duties of the post;	YES ☐	NO ☐
Have a thorough knowledge of one of the official EU languages and a satisfactory knowledge (at least at the B2 level or equivalent) of another of these languages to the extent necessary for the performance of their duties (candidates are invited to specify in their CV possible language certificates they have obtained and which can demonstrate their language skills).	YES ☐	NO ☐
Be physically fit to perform the duties linked to the post. Before being engaged, a member of the temporary staff shall be medically examined by one of the institution's medical officers in line with the requirement of Art. 12(2) (d) of the Conditions of Employment of Other Servants (CEOS).	YES ☐	NO ☐

SELECTION CRITERIA

A. Essential

A University degree on Information and Technology, Engineering/Science, Computer Science, Cybersecurity or any other domain that is deemed relevant to the post.	**YES**	**NO**
	☐	☐

If so, please indicate the degree and the university as well as number of years and subjects related to this job description (300 words maximum)

Minimum 5 years of professional experience with tasks closely related to those described in section '2. Job Description – Duties and responsibilities'.	**YES**	**NO**
	☐	☐

If so, please describe the business context, the project/activity, the nature of your work, your exact role and responsibilities and the tangible results of your work (300 words maximum)

Professional experience with security aspects of ICT systems, preferably for processing of classified information;	**YES**	**NO**
	☐	☐
If so, please describe the business context, the project/activity, the nature of your work, your exact role and responsibilities and the tangible results of your work (300 words maximum);		

Excellent written and oral communication skills, with demonstrated ability to communicate administrative, financial and business information at all levels inside and outside the organization;	**YES**	**NO**
	☐	☐
If so, please give examples during your career where you proved this skill (300 words maximum);		

Excellent command of written and spoken English.	**YES**	**NO**
	☐	☐
If so, please give examples during your career where you proved this skill (300 words maximum);		

B. Advantageous

Working experience in a field related to the duties in an international and multicultural environment, preferably within a European Institution or body.	**YES**	**NO**
	☐	☐
If so, please describe the business context, the project/activity, the nature of your work, your exact role and responsibilities and the tangible results of your work (300 words maximum)		

Practical experience/knowledge of European Commission IT systems and procedures.	**YES**	**NO**
	☐	☐
If so, please describe where and how you acquired it and specify the IT tools (300 words maximum);		

MOTIVATION LETTER
Why do you want to apply for this career opportunity? What specific contribution do you think you could make to ECCC? (500 words maximum)

Declaration: I declare on my honour, that the information provided above is true, complete and correct.

Date:…….. Signature:……