

# CALL FOR EXPRESSIONS OF INTEREST FOR CONTRACT STAFF

## IN THE FIELD OF ICT SECURITY Function Group III: ICT Security Assistant Function group IV: ICT Security Analyst

**EPSO/CAST/S/7/2013**

### I. INTRODUCTION

At the request of the European Union institutions, the European Personnel Selection Office (EPSO) is launching a selection procedure to set up a database of successful candidates from which to recruit contract staff in the field of **ICT** (Information and Communications Technology) **and Cyber Security**.

The institutions of the European Union recruit contract staff to provide additional capacity in specialised fields. Contract staff are employed in accordance with the conditions given in section IX of this call for expressions of interest.

The working relationship with the European institutions is governed by the Conditions of Employment of Other Servants of the European Union. The working conditions can be found in full online at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1962R0031:20100101:EN:PDF> (chapter IV, page 172)<sup>1</sup>.

The database will be used by the European Commission, the European Parliament, the General Secretariat of the Council, the European External Action Service and the Economic and Social Committee. **The functions will mainly be based in Brussels and Luxembourg as required. A limited number of jobs could be located in some of the EU Delegations around the world.**

Selection procedures for contract staff usually attract a large number of highly qualified candidates who are successful in the selection procedure. Therefore, candidates should be aware that for certain profiles it is possible that the number of names in the database will be greater than the needs of the institutions.

The table below shows the institutions' estimated needs for contract staff in this field for a particular period of time taking into account the limited nature of the contracts and staff rotation.

Approximate size of the pool of successful candidates required by the institutions over the three-year period 2014-2016:

Function group	Profile	Number
FGIII	ICT Security Assistant	50
FGIV	ICT Security Analyst	50

**Candidates may register for one profile and one function group only. However, should candidates who apply for function group IV (FGIV) fail to obtain the pass mark for this function group in the competency test they may be reclassified, with their prior agreement, in function group III (FGIII) provided that they obtain the pass mark for function group III (please see details under point "VI. Selection phases")**  
**Candidates who make more than one application will be disqualified.**

<sup>1</sup> The general implementing provisions governing the conditions of employment for contract staff employed by the European Commission and the European Parliament can be found on EPSO's website.

## II. NATURE OF DUTIES<sup>2</sup>

### **FG III – ICT Security Assistant**

Under the supervision of an official or a temporary agent, the contract staff member will assist in handling announcements, coordinating alerts and incident response, carrying out forensic investigations and ICT security audits, managing ICT security infrastructure, defining ICT security configuration settings and drafting ICT security policies, standards and guidelines.

By way of example, the duties may include:

- Assist in implementing security solutions (infrastructure and/or application) including the design, configuration, development, testing and deployment of security-related technologies such as next generation firewalls, application firewalls, Identity & Access Management, IDS/IPS, Data Loss Prevention, Digital Rights Management, Network Access Control, Security Information & Event Monitoring (SIEM).
- Assist in information security awareness and training initiatives to educate workforce about information risks by providing orientation, educational programs, and on-going communication.
- Assist in designing, documenting and testing ICT process controls in a wide range of environments.
- Assist in audit and reviews of information security issues in the EU institutions.
- Assist in providing support to users or constituencies in security-related queries. Writing guidelines and support documents to upgrade defence lines.
- Assist in implementing, managing, and enforcing ICT security policies, guidelines and procedures inside the EU institutions.
- Act as duty officer in an incident response team, analysing incoming information on threats and compromised systems, prioritising information, designing announcements and alerts and sending them to the appropriate target audience.
- Assist in handling Information Security Incidents, assessing incoming information on incidents and taking appropriate action.
- Assist in ICT security forensic investigation and/or performing collection and analysis of artefacts.
- Assist in investigating instances of malicious code to determine attack vector, payload, and the extent of damage and data exfiltration.
- Assist in implementing security solutions for malicious activity intelligence gathering as well as collecting, managing and sharing intelligence on suspected malicious activity.
- Assist in investigating suspected and actual breaches of security and undertaking/reporting remedial action as required. Maintaining a log of any incidents and remedial recommendations and actions.
- Deploy, configure, administer and maintain cryptography systems.
- Deploy, configure, administer and maintain classified infrastructure/networks.
- Apply/enforce or audit ICT security policies.

### **FG IV – ICT Security Analyst**

Under the supervision of an official or a temporary agent, the contract staff member will take on conceptual work, analysis and technical and administrative supervision in the area of ICT support and infrastructure.

The contract staff member will carry out duties related to the management of announcements, alerts and incident response coordination, forensic investigations, ICT security audits, management of ICT security infrastructure, definition of ICT security configuration settings, drafting ICT security policies, standards and guidelines. Among other things these duties require an aptitude for drafting, analysis, technical supervision, administrative management and a thorough working knowledge of office software.

By way of example, the duties may include:

---

<sup>2</sup> The profiles described in this Call for expressions of interest are simplified versions of the generic profiles that will be used when drawing up contracts. These simplified versions are provided for information purposes and are not legally binding.

- Manage, coordinate and implement security solutions (infrastructure and/or application) including the design, configuration, development, testing and deployment of security-related technologies, next generation firewalls, application firewalls, Identity & Access Management, IDS/IPS, Data Loss Prevention, Digital Rights Management, Network Access Control, Security Information & Event Monitoring (SIEM).
- Initiate information security awareness and training initiatives to educate workforce about information risks by providing orientation, educational programs, and on-going communication. Design, document and test ICT process controls in a wide range of environments.
- Manage ICT security project management including project planning, product evaluation, system/vendor selections, infrastructure design, readiness assessments, and quality assurance.
- Manage and coordinate audits and reviews of information security issues in the EU institutions.
- Handle and coordinate responses to information security incidents.
- Lead an incident response team to contain, investigate, and prevent future computer security breaches.
- Develop, implement and enforce suitable and relevant information security policies and ensuring that these are compliant with the EU Data Protection Directive and other legislation and regulations related to information security; reviewing policies on a regular basis.
- Ensure the integration of information security with business strategies and requirements.
- Coordinate ICT security forensic investigation and/or collection and analysis of artefacts.
- Investigate instances of malicious code to determine attack vector, payload, and to determine the extent of damage and data exfiltration.
- Manage, coordinate and implement security solutions for malicious activity intelligence gathering, as well as collecting, managing and sharing intelligence on suspected malicious activity.
- Conduct security research in keeping abreast of latest security issues.
- Work with vendors, external consultants, and other third parties to improve information security within the EU institutions.
- Manage the integration of information security systems into the business environment.
- Analyse, evaluate and improve ICT tools, processes, working procedures and methods in the area of ICT Security.
- Design, deploy, configure, administer and maintain cryptography systems.
- Design, deploy, configure, administer and maintain classified infrastructure/ networks.
- Propose, apply/enforce and/or audit ICT security policies.

### III. INDICATIVE TIMETABLE OF THE SELECTION PROCEDURE

The procedure will be administered by EPSO with the assistance of a selection panel comprised of representatives from departments of the EU institutions. The **indicative** timetable is as follows:

STEP	Indicative dates
CV sifting	September 2013
Competency test	November 2013
Results of the competency test	December 2013-January 2014

## IV. ELIGIBILITY REQUIREMENTS

On the closing date for online applications you must fulfil the following conditions:

<b>A. General conditions</b>	
a) be a citizen of one of the Member States of the European Union at the closing date for online applications	
b) enjoy your full rights as a citizen	
c) have fulfilled any obligations imposed on you by the laws on military service	
d) meet the character requirements for the duties involved.	
<b>B. Minimum specific conditions - Education/experience</b>	
<b>FG III – ICT Security Assistant</b>	
<ul style="list-style-type: none"> <li>A level of post-secondary education, attested by a diploma, in a technical field related to the duties described in Section II, or</li> <li>A level of secondary education attested by a diploma giving access to post-secondary education followed by 3 years' professional experience related to the duties described in Section II.</li> </ul>	
<b>FG IV - ICT Security Analyst</b>	
Completed university studies of at least 3 years attested by a diploma in a field related to the duties described in Section II.	
<b>C. Knowledge of languages</b>	
a) Language 1 (L1) and b) Language 2 (L2)	<p>Main language: thorough knowledge of one of the official languages of the European Union<sup>3</sup></p> <p>A satisfactory knowledge (level B2<sup>4</sup>) of English, French or German; must be different from language 1 above.</p> <p>In conformity with the judgment rendered by the EU Court (Grand Chamber) in Case C-566/10 P, Italian Republic v Commission, the EU institutions are required to state the reasons for limiting the choice of the second language in this selection to a restricted number of EU official languages.</p> <p>Candidates are therefore informed that the second language options in the present selection have been defined in accordance with the interest of the service which requires that newly recruited colleagues are immediately operational and able to communicate efficiently in their daily work. Otherwise the effective functioning of the institutions would be severely impaired.</p> <p>On the basis of a long-standing practice of the EU Institutions as regards the languages used for internal communication and also taking into account the needs of the services regarding external communication and handling of files, English, French and German remain the most widely used. Moreover, English, French and German are the second languages by far the most widely chosen by the candidates of selections where they have a free choice. This confirms</p>

<sup>3</sup> The official languages of the European Union are: BG (Bulgarian), HR (Croat), CS (Czech), DA (Danish), DE (German), EL (Greek), EN (English), ES (Spanish), ET (Estonian), FI (Finnish), FR (French), GA (Irish), HU (Hungarian), IT (Italian), LT (Lithuanian), LV (Latvian), MT (Maltese), NL (Dutch), PL (Polish), PT (Portuguese), RO (Romanian), SK (Slovakian), SL (Slovenian), SV (Swedish).

<sup>4</sup> See the reference grid on the Europass website at the following address:

[http://europass.cedefop.europa.eu/europass/home/hornav/Downloads/CEF/LanguageSelfAssessmentGrid.csp?loc=en\\_EN](http://europass.cedefop.europa.eu/europass/home/hornav/Downloads/CEF/LanguageSelfAssessmentGrid.csp?loc=en_EN)

	current educational and professional standards, whereby candidates for European Union positions can be deemed to master at least one of these languages. Therefore, in balancing the interest of the service and the needs and capacities of the candidates by also taking account of the particular field of this selection, it is legitimate to organise tests in these three languages in order to ensure that, whatever their first official language, all candidates master at least one of these three official languages at working level. Moreover, in the interest of equal treatment of all candidates, everyone, including those whose first official language is one of these three, is required to take the test in his or her <u>second</u> language, chosen from among these three. Assessment of specific competences in this way allows the Institutions to evaluate the ability of candidates to immediately perform in an environment that closely matches the reality they would face on the job. This is without prejudice to later language training so as to acquire a capacity to work in a third language in accordance with Art. 85(3) of the CEOS.
--	---

You may apply for only one of the 24 official languages as your main language (L1). You will not be able to change your choice of languages once you have validated your online application form.

**Note: If you are invited to an interview, you will have to submit all supporting documents. If it is found that the information you provided is incorrect, you will be excluded from the selection procedure and your name will be removed from the database.**

## V. HOW TO APPLY AND DEADLINE FOR APPLYING

You must apply online by following the instructions on the EPSO website ([http://europa.eu/epso/apply/jobs/index\\_en.htm](http://europa.eu/epso/apply/jobs/index_en.htm)), and particularly in the online application manual. You must fill in the application form in English, French or German.

The responsibility for completing your on-line application before the deadline is entirely yours. We advise you not to wait until the last minute before applying, since if the lines are exceptionally busy or the Internet connection goes down, you may have to repeat the whole on-line application process and once the deadline has passed, you will no longer be able to do so.

Once you have validated your application, you will no longer be able to make any changes; the data entered are immediately processed by EPSO with a view to organising the selection procedure.

### **DEADLINE (including validation)**

**16/07/2013 at 12:00 (midday) Brussels time**

## VI. SELECTION PHASES

### SELECTION BASED ON QUALIFICATIONS

Candidates will be screened on the basis of their qualifications, particularly in terms of their diplomas and professional experience, against the criteria set out below, and those whose profiles best match the duties and the selection criteria will be invited to the competency test.

A selection panel will be appointed to assist EPSO at this stage of the selection procedure, specifically to carry out the selection based on qualifications (CV sifting).

### **Criteria for selection based on qualifications**

#### **FG III – ICT Security Assistant**

1. After having obtained a diploma of post-secondary education, professional experience of at least 3 years in the field of ICT Security or Cyber Security
2. If you have only obtained a diploma of secondary education followed by experience of 3 years related to the duties, additional professional experience of at least 3 years in the field of ICT Security or Cyber Security
3. Irrespective of the diploma obtained and as part of your professional experience under points 1 or 2 above, experience of at least 6 months that is specifically related to the duties described under point II " Nature of duties" of this Call
4. ICT Security or Cyber Security certification, such as CISSP, GIAC, etc.
5. Training (other than that mentioned under the eligibility requirements, point IV.B., of this Call) in the field of ICT Security and Cyber Security
6. Active involvement in the development of ICT Security Projects
7. Contribution to development of ICT standards (e.g. IETF)
8. Experience in working as a member of an incident response team
9. Experience in working as a member of a secure communications team
10. Experience in working with classified ICT security systems
11. Good knowledge of English (even if language 1 or 2) (at least level B2<sup>5</sup>)

#### **FG IV – ICT Security Analyst**

1. After having obtained the university degree, professional experience of at least 5 years in the field of ICT Security or Cyber Security
2. As part of your professional experience under point 1, experience of at least 6 months that is specifically related to the duties described under point II " Nature of duties" of this Call
3. ICT Security or Cyber Security certification, such as CISSP, GIAC, etc.
4. Training (other than that mentioned under the eligibility requirements, point IV.B., of this Call) in the field of ICT Security and Cyber Security
5. Active involvement in the development of ICT Security Projects
6. Contribution to development of ICT standards (e.g. IETF)
7. Experience in working as a member of an incident response team
8. Experience in working as a member of a secure communications team
9. Experience in working with classified ICT security systems
10. Proficient knowledge of English (even if language 1 or 2) (at least level C1<sup>6</sup>)
11. Publications on ICT Security or Cyber Security i.e. conference proceedings, scientific journals or books

**Note: If you are invited to an interview, you will have to submit all supporting documents. If it is found that the information you provided is incorrect, you will be excluded from the selection procedure and your name will be removed from the database.**

The selection based on qualifications is carried out **solely** on the basis of the information provided by the candidate in the 'Talent Screener' tab of the application form and takes place in two stages:

— Stage 1: An initial selection based on qualifications will be made on the basis of the responses (yes/no) ticked by the candidate and the weighting assigned to each question, which will be on a

---

<sup>5</sup> See the reference grid on the Europass website at the following address:

[http://europass.cedefop.europa.eu/europass/home/hornav/Downloads/CEF/LanguageSelfAssessmentGrid.csp?loc=en\\_EN](http://europass.cedefop.europa.eu/europass/home/hornav/Downloads/CEF/LanguageSelfAssessmentGrid.csp?loc=en_EN)

<sup>6</sup> See the reference grid on the Europass website at the following address:

[http://europass.cedefop.europa.eu/europass/home/hornav/Downloads/CEF/LanguageSelfAssessmentGrid.csp?loc=en\\_EN](http://europass.cedefop.europa.eu/europass/home/hornav/Downloads/CEF/LanguageSelfAssessmentGrid.csp?loc=en_EN)

scale of 1 to 3 according to the importance attached to the corresponding criterion. The candidates who obtain the highest number of points will go through to the second selection stage (about five times the number of candidates, per profile, required by the institutions).

- Stage 2: The selection panel will scrutinise candidates' responses and will award 0 to 4 points for each response; the points are then multiplied by the weighting assigned to the corresponding criterion.

The candidates who obtain the highest number of points will be invited to the competency test (about 2 and a half times the number of candidates, per profile, required by the institutions). Where a number of candidates tie for the last available place, they will all be invited to the competency test.

### COMPETENCY TEST

Candidates will sit a competency test to assess their knowledge in the chosen profile.

Tests for function groups III and IV will be the same but pass marks will be different for each function group as outlined in the table below. With their prior agreement (to be stated in the application form), candidates who apply for FG IV who do not obtain the required pass mark will be reclassified in function group III, provided that they obtain the pass mark for function group III. For both function groups, candidates who do not reach the pass mark will fail.

Test type	Time allowed for test	Language of the test	Maximum number of points	Minimum score required	
Multiple choice	50 minutes	Language 2 (L2)	25	FG III	FGIV
				13	16

The test will be either paper-based and held for all candidates in Brussels, or computer-based and held in test centres throughout the member states. Candidates will be informed of the arrangements chosen in due course.

If the tests are paper-based and held for all candidates in Brussels, EPSO will pay an allowance for travel expenses in line with the relevant rules on reimbursement, which can be found on EPSO's website at [http://europa.eu/epso/apply/on\\_going\\_compet/reimburse/index\\_en.htm](http://europa.eu/epso/apply/on_going_compet/reimburse/index_en.htm).

## **VII. TEST RESULTS**

The CV sifting and competency tests results will be published in the candidates' EPSO accounts.

## **VIII. INCLUSION IN THE DATABASE**

The names of candidates who obtain the pass mark in the competency test will be entered in a database and will not be made public in any other form. Access to the database will be granted to the European Commission, the European Parliament, the General Secretariat of the Council, the European External Action Service and the Economic and Social Committee. Other European Institutions/Agencies may also obtain access should they have a need for these profiles. The database will remain valid for a period of three years from the date when candidates are notified of their results.

The European Commission has begun negotiations for the amendment of the Staff Regulations for Officials and the Conditions of Employment of Other Servants of the European Union. The amendment may concern the careers of officials and other servants. Candidates included in the database of this selection procedure may receive a job offer based on the new provisions of the Staff Regulations once they have been adopted by the legislator without prejudice to other consequences of a legal or financial nature.

## IX. SELECTION FOR POTENTIAL RECRUITMENT

**Inclusion in the database is not a guarantee that you will be offered a job.** As vacancies arise, institutions will search the database and invite for an interview those candidates who best match the job requirements in question; depending on the outcome, they may then make a formal job offer. Your knowledge of your main language will also be assessed during this interview. If applicants do not already possess a Personnel Security Clearance (PSC) they accept to submit a formal request immediately after recruitment. The applicant chosen for a position will be offered either a CA 3A<sup>7</sup> or a CA 3B<sup>8</sup> contract, depending on the employer making the job offer, as indicated below.

Contract	Place of activity
CA 3B (fixed-term)	Commission Directorates-General (except the Offices), the European Parliament, the General Secretariat of the Council, the European External Action Service (except EU delegations) and the Economic and Social Committee, European Anti-Fraud Office (OLAF) and the Publications Office of the European Union (OP)
CA 3A (could lead to an indefinite contract)	Commission: The two Offices for Infrastructure and Logistics in Brussels and Luxembourg, the Paymasters Office (PMO); the European Personnel Selection Office (EPSO) and the European School of Administration (EUSA), European agencies and Commission Representations and European Union Delegations in the world.

## X. REVIEW/APPEAL PROCEDURES

### X. 1. APPEALS

If at any stage of this selection procedure you consider that a mistake has been made or that EPSO has acted unfairly or has failed to comply with the rules governing this selection procedure, and that your interests have been prejudiced as a result, the following appeal procedures can be undertaken in the order mentioned in the table below:

Procedure	Contact point	Time limit <sup>9</sup>
1. Request a review	Via the contact page on EPSO's website	10 calendar days
2. Lodge an administrative complaint under Article 90(2) of the Staff Regulations of Officials of the European Union <sup>10</sup>	Either by post to: European Personnel Selection Office (EPSO) C-25, 1049 Brussels, Belgium or via the contact page on EPSO's website	3 months
<b>After completion of step 2 above (step 1 is optional) you have the possibility to:</b>		
3. If your complaint is rejected explicitly or tacitly, submit a judicial appeal under Article 270 of the Treaty on the Functioning of the European Union and	European Union Civil Service Tribunal Boulevard Konrad Adenauer 2925 Luxembourg	3 months

<sup>7</sup> Under Article 3a of the Conditions of Employment of Other Servants of the European Union (CEOS) and under the conditions laid down by the CEOS and the General Implementing Provisions of the institution, agency or office.

<sup>8</sup> Under Article 3b of the Conditions of Employment of Other Servants of the European Union (CEOS) and under the conditions laid down by the CEOS and the General Implementing Provisions of the institution, agency or office.

<sup>9</sup> From the date of publication of the decision in the candidate's EPSO Account.

<sup>10</sup> Please quote the following in the subject line of your letter: Selection number; your application number; and 'Complaint under Article 90(2)'.



Like all citizens of the European Union, you can make a complaint to the European Ombudsman:

European Ombudsman  
1 avenue du Président Robert Schuman —  
CS 30403  
67001 Strasbourg Cedex  
FRANCE<sup>12</sup>

## X.2. REQUESTS FOR CORRECTIVE MEASURES

If you consider that one or more of the questions put to you in the tests contained an error such as to make it impossible to answer or such as to affect your ability to answer correctly, you are entitled to inform EPSO, who will take, after verification, possible corrective measures.

Requests for corrective measures must be made **within 10 calendar days of the date of your test** via the functional mailbox [EPSO-CAST-S-7-2013@ec.europa.eu](mailto:EPSO-CAST-S-7-2013@ec.europa.eu).

In your request, you **must** provide your candidate number and the information necessary to identify the question(s) that you believe contained errors (for example by describing what the question was about and/or mentioning the question number), and explain as clearly as possible the nature of the alleged error.

**Requests received after the deadline or which are not clear enough to help identify the question(s) contested will not be taken into account.**

## XI. COMMUNICATION

EPSO will contact you via your EPSO account. It is up to you to consult your EPSO account at regular intervals — at least twice a week — to keep track of the progress of the procedure and to check the information relevant to your application. If you are prevented from doing so because of a technical problem that is attributable to EPSO, you must notify EPSO immediately.

For all correspondence with EPSO, please use the contact form on the EPSO website at: <http://blogs.ec.europa.eu/eu-careers.info/cast/>.

To ensure that all general texts and all communication between you and EPSO are clearly understood on both sides, only English, French, or German will be used for the invitations to the various tests and correspondence between you and EPSO.

## XII. GROUNDS FOR DISQUALIFICATION LINKED TO THE APPLICATION PROCESS

<sup>11</sup> For details of how to submit an appeal and calculation of the time limits, please consult the website of the European Union Civil Service Tribunal at: [http://curia.europa.eu/jcms/jcms/T5\\_5230](http://curia.europa.eu/jcms/jcms/T5_5230).

<sup>12</sup> 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 Civil Service Tribunal under Article 270 of the Treaty on the Functioning of the European Union. 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. For full details of the procedure, consult the website at: <http://www.ombudsman.europa.eu/en/home>.

EPSO takes great care to see that the principle of equal treatment is observed. Consequently, if at any stage in the procedure EPSO finds that you have created more than one EPSO account, made more than one application to this selection procedure or that you have made any false declarations, you will be disqualified.

Fraud or attempted fraud may render you liable to penalty. We would point out that anyone recruited by the institutions must show themselves to be of the highest possible integrity.

### **XIII. SPECIAL ARRANGEMENTS FOR CANDIDATES WITH DISABILITIES**

#### a) Condition existing at time of application

1.	If you have a disability or a condition that might pose difficulties for you when taking the tests, tick the corresponding box on the online application form and indicate what arrangements you consider necessary to make it easier for you to take the tests, quoting the number of the selection procedure and your application number (be sure not to omit these).
2.	Send either a medical certificate or a certificate attesting your disability issued by a recognised body (whichever is appropriate) as soon as possible after validating your online application. These supporting documents will be examined so that special arrangements to suit each case can be made in order to satisfy (as far as possible) requests that are judged to be reasonable. Requests and supporting documents should be sent: either by e-mail to: EPSO-accessibility@ec.europa.eu, or by fax to: +32 22998081, addressed to 'EPSO accessibility', or by post to: European Personnel Selection Office (EPSO) 'EPSO accessibility' (C-25) 1049 Bruxelles/Brussel BELGIUM

#### b) Condition developing after application

1.	If a condition of the kind described above develops after the deadline for online applications, you must inform EPSO as soon as possible. Please state in writing what arrangements you consider necessary.
2.	Send the relevant documents either by e-mail to: EPSO-accessibility@ec.europa.eu, or by fax to: +32 22998081, addressed to 'EPSO accessibility', or by post to: European Personnel Selection Office (EPSO) 'EPSO accessibility' (C-25) 1049 Bruxelles/Brussel BELGIUM