

SELECTION NOTICE FOR SECURITY OFFICER – CYBERSECURITY

REFERENCE NUMBER: ACER/2023/08

Position (job title):	Security Officer – Cybersecurity
Department / Team:	Coordination, Operations and Legal Department
Function Group / Grade:	Temporary Staff AD6 / This Selection Notice is published at a single grade
Contract duration	5 years (with possibility of renewal)
Place of employment:	Ljubljana, Slovenia
Starting date:	Spring 2024
Closing date for applications:	15 January 2024, 14:00 Ljubljana time

1. ABOUT THE AGENCY

The European Union Agency for the Cooperation of Energy Regulators (hereinafter referred to as “ACER”) is a European Union (“EU”) body, legally established by Regulation (EU) No 2019/942¹ and operational since 2011. ACER is central to the integration and well-functioning of the EU's electricity and natural gas markets.

1.1 Our purpose

Our overall purpose is achieving a transition of the European energy system in line with the political objectives set, reaping benefits of increased energy market integration across Europe, and securing low-carbon supply at least possible cost for European businesses and citizens.

The Agency promotes:

- A more competitive, integrated market, offering consumers more choice;
- An efficient energy infrastructure and network, enabling energy to move freely across borders, the integration of renewable sources, and therefore ensuring a higher degree of security of supply;
- A monitored and transparent energy market guaranteeing consumers fair prices and limitation of market abusive behaviours.

In this respect, ACER:

- Complements and coordinates the work of NRAs;
- Participates in the development of European network rules;
- Takes, under certain conditions, binding individual decisions on terms and conditions for access and operational security for cross-border infrastructure, on cross-border cost allocation for Projects of Common Interest and on terms and conditions or methodologies for the implementation of network codes;
- Gives advice on electricity and natural gas related issues to the European institutions;
- Monitors the internal markets in electricity and natural gas and reports on its findings;

¹ Regulation (EU) No 2019/942 of the European Parliament and of the Council of 05 June 2019 (recast).

- Monitors trading in wholesale energy products to detect and deter market abuse and ensure the integrity and transparency of EU wholesale energy markets in accordance with REMIT i.e., Regulation (EU) No 1227/2011.

1.2 ACER's evolving role

ACER is on a significant growth trajectory, marked by an expanding number and array of tasks in the recent years. Our role as a collaborative agency within the framework of the EU's national energy regulatory authorities remains at the heart of our mission, complimented by a range of tasks that span various aspects of the EU energy system, encompassing monitoring of energy flows, wider system needs, and so much more.

ACER is currently at a critical point, playing a key role in advancing EU energy market integration and bolstering market integrity and transparency; efforts that strike us as more crucial than ever. Our goal is to contribute with our capacities, insights, and creativity as an EU energy regulatory agency to a transition of the energy system that is affordable, secure, and decarbonized – a transition that takes place at the pace set by leaders across the EU.

ACER has been entrusted with additional responsibilities under the "Clean Energy for all Europeans" legislative package, and is expecting new legislative packages to be adopted, focusing on key areas such as Gas Decarbonisation, REMIT reform, and Electricity Market Design, aiming to bring transformative changes and further evolving the European energy landscape.

1.3 Who we are

ACER currently employs around 175 staff (statutory and non-statutory) and has an approved annual budget of € 32,602,073 in 2024. With the new responsibilities being assigned to its mandate, the Agency anticipates a significant growth in the forthcoming years, expecting more than 200 staff by 2025.

Our organizational structure is undergoing a transformation to enhance our efficiency and effectiveness. We are in the process of finalizing a reorganization that will result in the following new structure, comprising seven Departments in 2024: Coordination, Operations and Legal, Electricity, Energy system needs, Gas Hydrogen and Retail, Market Information and Transparency, Market Surveillance and Conduct, REMIT Investigation.

1.4 Our ongoing journey of progress

ACER offers a dynamic and motivating workplace, where diversity is celebrated and where people's commitment and achievements contribute to build an organisation that is better than the sum of its parts. We strive towards becoming an innovative and engaging workplace, by committing continuously to invest in learning and development opportunities and by focusing on staff well-being and work-life balance.

We invest heavily in the professional development of staff, support a 'low on hierarchy, high on impact' organisational culture, prioritise personal relations and support an active constructive feedback culture, emphasising the positives whilst not shying away from addressing the negatives.

Looking ahead, as a growing agency we recognize the importance of focusing on cross-organizational issues, encompassing both work practices and our broader work culture. We find this essential to maintain a cohesive, collegial work culture ("one ACER"), which is reinforced as we welcome a significant number of new colleagues joining our agency in the coming years.

At ACER we believe in fostering a high-impact, high-performance type of environment, built on strong mutual trust, empowerment, personal responsibility, psychological safety, and teamwork at all levels.

2. WHAT WE LOOK FOR

2.1 The profile

We are looking for a **Security Officer – Cybersecurity** to join our team. The Security Officer's focus will not only be limited to the assessment whether risks and vulnerabilities exist but also how those

could be mitigated with the aim to help provide the organisation with more confidence about system stability going forward. We value individuals who demonstrate a passion, interest, curiosity and strong devotion to continuously develop oneself in these areas. Key attributes include a focus on collaborating across the organization, and proactively addressing challenges, by tackling subpar output or approaches in a manner that brings results.

The jobholder will work under the responsibility of the Head of the Coordination, Operations and Legal Department and report directly to the Chief Information Security Officer, who is in charge of ensuring that ACER personnel, information, buildings and equipment are adequately protected against threats to their security and that security rules are respected and implemented. The Security Officer - Cybersecurity will support the information security coordination in establishing the assurance that ACER information systems will protect the information they handle, under the control of legitimate users.

We are committed to continually enhancing our operational processes, which may involve modifying or reallocating specific responsibilities. It is imperative that our Security Officer – Cybersecurity exhibit flexibility, openness to change, and the ability to adapt to evolving roles.

2.2 Competencies

All staff working at ACER share the following **core competencies**:

- **Cooperating:** working with others towards achieving work goals;
- **Delivering quality results:** focusing on achieving results while applying relevant processes and procedures to meet quality standards;
- **Communicating:** sharing relevant information clearly and concisely, sharing useful information with others as appropriate;
- **Problem solving:** having the ability to identify and raise issues or concerns and seeking to anticipate problems a positive and helpful manner;
- **Being service oriented:** complying with ACER's rules and procedures, providing support and delivering services with a view to provide added value;
- **Self-development and knowledge sharing:** ability to share knowledge to support team effectiveness, while seeking feedback to enhance own performance;
- **Valuing diversity:** welcoming and working respectfully, inclusively and effectively with people from diverse backgrounds, while demonstrating respect and understanding of different points of view.

Security Officer – Cybersecurity will be required to have the following **specific / functional competencies**:

- **Having Technical Expertise:** provide advice in their area of expertise on the development and application of professional and scientific methods, procedures and approaches, ensure that work adheres to accepted technical standards and scientific methods; keep abreast of the latest developments in the field of their expertise, act as a technical/scientific resource and support the development of new colleagues;
- **Having Knowledge and Skill in regulations and procedures:** understanding EU policies and processes, having knowledge of the tasks and main documents of the Agency;
- **Managing projects :** define, plan, prepare, manage and execute projects, close and evaluate projects.

2.3 The position

Security Officer – Cybersecurity will become part of a diverse, young, and motivated team of approximately 36 people coming from 13 different Member States.

The **Security Officer – Cybersecurity** will be using his/her skills to detect unsecure aspects and malicious activities within our systems, policies and procedures. He/She will implement customized

application security assessments for asset risk, corporate policy compliance as well as conduct vulnerability assessments and penetration tests potentially with the assistance of contractors. **The main purpose of the job** is to contribute to the activities of the Agency in the field of Cybersecurity and ensure adequate controls and measures are in place so that all data, information systems and assets are protected against cyber risks.

Main responsibilities

The duties of the Security Officer – Cybersecurity will include the following:

- Improve and retain the policies and procedures related to information security to the highest standards;
- Exhibit a service-oriented mindset keeping in mind the interest of the service, as well as the interest of our internal & external stakeholders;
- Be an every-day champion of ACER's values (Cooperating, Delivering Quality Results, Communicating, Problem Solving, Being Service Oriented, Self-development & Knowledge Sharing, Valuing Diversity & Inclusion), while delivering all the tasks and duties pertinent with the role;
- Compile policy papers, informative reports and briefing notes in accordance with the respective competency areas;
- Offer credible advice and practical guidance to the various stakeholders across the organization with regard to information security;
- Contribute to the management and implementation of information security related projects, including the implementation of cybersecurity tools;
- Develop and retain a Business Continuity Plan of ACER taking into consideration the current and future mandate of the Agency;
- Provide support in creating documents and record management systems at ACER;
- Conduct security evaluation, inspection, monitoring, reviews, and audits connected to information systems;
- Establish mechanisms and procedures which can assure that information risks are managed with prudence and effectiveness;
- Be proactive and ensure that the information security systems are fully compliant with ACER security policies, standards, procedures and guidelines;
- Collaborate with the operations and IT departments, offer advice and guidance to identify pertinent security assessments;
- Be the liaison with the national and EU security authorities and services on information security matters of the Agency;
- Deliver awareness sessions on information security topics, risks, threats, vulnerabilities and best practice to ACER Senior Management and employees;
- Coordinate and support the information security governance and management bodies, including the Security Committee;
- Support the tasks associated with Data Protection;
- Cooperate closely with other teams and departments to validate and govern the implementation of security policies and programs, and
- Be willing to assume any other duties in the area of competence based on the existent business needs and as assigned by the Business Manager.

The Security Officer – Cybersecurity may be required to work in other areas of ACER, according to needs and priorities, as determined by the Director.

3. WHAT WE OFFER

3.1 What you can expect in the role

- Committed and motivated teammates by your side with the aim to excel in the assigned deliverables;
- To develop, and to be positively challenged and grow, in your role both in the team and in the whole of the organization;
- To be given the opportunity to harness your strengths while also receiving support in addressing any weaknesses or areas of improvement you may have;
- To be a part of an evolving team aiming for rapid maturity growth and thus offering a blend of constructive challenges and support, ultimately contributing to your professional growth and the collective betterment of the cybersecurity of the Agency;
- External collaboration with the European Commission, the European Parliament, the Council, or EU agencies like ENISA, CERT-EU and others.

3.2 Work-life balance

At ACER, we are committed to providing a healthy work-life balance, by offering the possibility of hybrid working arrangements that allow you to balance your professional and personal life effectively. With flexible working hours, you can tailor your schedule to suit your preferences, making it easier to manage your commitments both in and outside of work. We believe that a harmonious work-life balance is essential for everyone's well-being and productivity.

3.3 Conditions of employment

Pursuant to Article 2(f) of the CEOS, the successful candidate will be appointed by the Director as a Temporary Staff in Grade AD 06 for a period of 5 years, which may be renewed.

Pay and welfare benefits: The pay of staff members consists of a basic salary, allowances and other benefits. Depending on the individual family situation and the place of origin, the successful jobholder may be entitled to expatriation allowance (16% of the basic salary), household allowance, dependent child allowance, education allowance, pre-school allowance, reimbursement of removal costs, daily subsistence allowance, installation allowance and other benefits. Salaries are exempted from national tax; a Union tax is paid at source.

Additional benefits:

- Annual leave entitlement of two days per calendar month plus additional days for age, grade, 2,5 days' home leave if applicable, and in addition up to 19 ACER holidays per year;
- EU Pension Scheme (after 10 years of service);
- EU Joint Sickness and Insurance Scheme (JSIS), accident and occupational disease coverage, unemployment and invalidity allowance and insurance.

An accredited [European School](#) operates in Ljubljana as of September 2018 to allow dependent children of all ACER statutory staff (including Slovene nationals) to attend a (tuition-free) European-type multilingual education. The school successfully established all of the Primary school levels (P1-P5), Secondary levels are currently available from S1 to S6, with the final S7 level being opened in September 2024/2025, when the first European Baccalaureate will be obtained.

In addition, in case the appropriate education level is not yet available for a child in the accredited European School, up to a certain ceiling, the Agency contributes to the tuition cost of each dependent child attending another international school in Ljubljana territory.

Estimation of monthly basic salary, with specific allowances where applicable:

Grade/Step	Monthly basic salary (gross)	Estimation of monthly net salary, including specific allowances ²
AD 6, Step 1	6.231,42 €	6,343.89 €

4. REQUIREMENTS

4.1 Eligibility criteria

Candidates will be considered eligible for the selection phase on the basis of the following formal criteria to be fulfilled by the deadline for applications:

- 1) To have a level of education which corresponds to completed university studies of at least three (3) years, attested by a diploma;
(Only study titles that have been awarded in the EU Member States or Norway, Iceland and Liechtenstein or that are subject to the equivalence certificates issued by the authorities in the said Member States shall be taken into consideration.)
- 2) By the closing date for applications candidates must, after obtaining the qualifications mentioned in point 3.A.1, have acquired at least three (3) years of appropriate professional experience³;
- 3) To have a thorough knowledge of one of the official languages of the European Union⁴ or Norway, Iceland and Liechtenstein and satisfactory knowledge of a second of these languages (level B2 of CEFR⁵) to the extent necessary to perform their duties;
- 4) To be a national of a Member State of the European Union, Norway, Iceland or Liechtenstein;
- 5) To be entitled to their full rights as a citizen;
- 6) To have fulfilled any obligations imposed by the applicable laws concerning military service;
- 7) To be physically fit to perform the duties linked to the post⁶.

4.2 Selection criteria

The following criteria will be assessed when selecting the candidates for the interviews:

Essential criteria (*minimum 0 and maximum 3 points per criterion*)

- 1) Relevant studies in the field of electrical engineering, computing sciences, physics, information technology, cybersecurity or similar;
- 2) By the deadline for applications, having acquired at least four (4) years of relevant professional experience in the area of cybersecurity, after obtaining the qualifications mentioned in point 4.1 1) above;
- 3) In-depth knowledge of cybersecurity policy and risk management frameworks of complex IT systems in medium-large organizations;

² An estimation of net salary, including the deduction for tax, correction coefficient (91.9% for Slovenia) and social security, adding the allowances (this estimation has been calculated with expatriation allowance, household allowance and with one dependent child allowance.

Please note that allowances depend in any case on the personal situation of the candidate.

³ Professional experience is considered only from the time the candidate obtained the diploma required for being eligible. At a later stage, the candidate will be asked to provide supporting documents confirming the length and the level of his/her professional experience.

⁴ The languages of the EU are Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, Irish, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovene, Spanish, and Swedish.

⁵ Language levels of the Common European Framework of Reference: <http://europass.cedefop.europa.eu/resources/european-language-levels-cefr>

⁶ Before the appointment, a successful candidate shall be medically examined by one of the institutions' medical officers in order for the Agency to be satisfied that he/she fulfils the requirement of article 28(e) of the Staff Regulations of the Officials of the European Union.

- 4) Sound knowledge and experience in Penetration Testing, Vulnerability Scanning and SIEM tools;
- 5) Sound knowledge of cybersecurity certifications and audit;
- 6) Sound knowledge of cybersecurity incident response processes or of cybersecurity crisis management;
- 7) Experience with Threat Hunting and Analysis.

Advantageous criteria (*minimum 0 and maximum 1 point per criterion*)

- 1) Experience with legal frameworks (i.e. GDPR) would be an advantage;
- 2) Experience with an EU institutional framework would be an advantage.

Candidates are invited to briefly explain in their application form in which positions they acquired their knowledge and professional experience in the specified areas.

5. SELECTION AND APPOINTMENT

A Selection Committee will evaluate the applications and select the candidates meeting the eligibility criteria and best matching the selection criteria.

The group of the highest scoring Applicants (hereinafter referred to as “Candidates”) shall be invited for a written examination and an oral interview with the Selection Committee.

The number of invited Candidates shall be, as a minimum, six.

The interview and test will focus on the following aspects.

- a) Specific competencies and knowledge of languages with reference to the selection criteria of the present selection notice;
- b) General aptitudes to the extent necessary for the performance of the duties in accordance with article 12.2.e of the Conditions of Employment of Other Servants (CEOS);

A reserve list of the most suitable candidates will be drawn up by the Agency.

In line with Director Decision 2023/24, candidates achieving the qualifying mark in the written test and interview of a minimum of 70% will be placed on the reserve list. The reserve list will be valid until 31/12/2024. Its validity may be extended by decision of the Director.

All candidates will be informed about the outcome of the procedure. Recruitment will be subject to budgetary availability and assignment of posts by the Budgetary Authority.

As part of our selection process, candidates will be asked to provide references from their former or current employments; for senior management positions, this would entail reference from a former or current superior, peer colleague, working at the same hierarchical level, and from a subordinate colleague.

6. EQUAL OPPORTUNITIES

The Agency applies an equal opportunities policy and accepts and treats applications without distinction on grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

ACER celebrates diversity! We are convinced that diversity is a strength in the workplace and that its harnessing will improve our productive environment, where everyone feels valued, where their talents are being fully empowered, and in which organisational goals are met.

The Agency is fully committed to the provision of equality of opportunity for all its employees through its employment practices, policies and procedures. ACER undertakes to provide a working environment that is sensitive to differences in racial or ethnic origin, religion or belief, disability, age, sexual orientation and gender. The Agency's way of working is based on a model of best practice whereby all employees can reach their full potential.

To this purpose, ACER applies a policy of equal opportunities and takes great care to avoid any form of discrimination in its selection and recruitment procedure: the Agency ensures that no employees nor job applicants is treated inequitably due to gender, marital or parental status, age, sexual orientation, disability, ethnicity, colour, citizenship/nationality or religious belief.

The Agency's premises are set to accommodate needs of persons with disabilities: ACER constantly makes sure to arrange what candidates, visitors and staff consider necessary to enable them to take part in the activities of the Agency.

The Agency offers a complete set of family support measures, from parental and family leaves to kindergarten and school support, better to foster the performance of duties for colleagues with caring responsibilities.

Work opportunities at ACER are open to nationals of the 27 European Union Member States. Currently the Agency employs staff from 26 different nationalities.

7. DATA PROTECTION

The purpose of processing the data that candidates submit is to manage their application(s) in view of possible (pre)selection and recruitment at the Agency. Personal data is processed by and accessible to authorised Agency's personnel. In some cases, an external expert, equally bound by the same data protection principles, may assist the Agency in the selection of candidates.

The Agency adheres to and is regulated by 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.

The Agency is supervised by EDPS (<http://www.edps.europa.eu>). For any further enquiries, candidates may contact the Data Protection Officer at DPO@acer.europa.eu. Candidates are invited to consult the privacy statement, which explains how the Agency processes personal data in relation to recruitment and selections, available on the Agency website.

8. HOW TO APPLY?

For applications to be valid, candidates must submit the following documents **in PDF**:

- A **complete and detailed curriculum vitae in English**;
- **Fully completed Application form** (Application forms that are incomplete, will not be taken into consideration)

Applications must be sent by e-mail 15/01/2024, 14:00h Ljubljana time.

Applications should be sent by email to SELECTIONS-ACER-2023-08@acer.europa.eu with the following **subject line: ACER-2023-08 NAME SURNAME**

Applications that are not complete or that are received after the deadline are considered as non-valid.

Supporting documents (e.g. certified copies of degrees/diplomas, references, proof of experience etc.) should not be sent at this stage but must be submitted at a later stage of the procedure if requested.

In order to facilitate the selection process, all communications to candidates concerning this selection will be in English.

Under no circumstances should candidates approach the Selection Committee, directly or indirectly, concerning this recruitment. ACER reserves the right to disqualify any candidate who disregards this instruction.

If at any stage in the procedure it is established that any of the information a candidate provided is incorrect, the candidate in question will be disqualified.

For more information on the selection procedure, please consult [ACER's website](#).

9. APPEALS

Pursuant to Article 90(2) of the Staff Regulations of Officials and the Conditions of Employment of Other Servants, a candidate may submit a complaint against an act affecting him/her adversely. The complaint must be lodged within three months from the date of notification to the following address:

Human Resources Management
European Union Agency for the Cooperation of Energy Regulators (ACER)
Trg Republike 3
1000 Ljubljana – Slovenia

Should the complaint be rejected, pursuant to Article 270 of the Treaty on the Functioning of the European Union and Article 91 of the Staff Regulations of Officials and the Conditions of Employment of Other Servants, a candidate may request judicial review of the act. The appeal must be lodged within three months from the date of notification to the following address:

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

Any citizen of the European Union or any natural or legal person residing in a Member State may make a complaint about maladministration pursuant to Article 228(1) of the Treaty on the Functioning of the European Union. The complaint must be lodged within two years of becoming aware of the facts on which the complaint is based on, to the following address:

The European Ombudsman
1, Avenue du President Robert Schuman - BP 403
F-67001 Strasbourg Cedex
France

Please note that complaints to the European Ombudsman do not have the effect of suspending the period mentioned in Articles 90 and 91 of the Staff Regulations of Officials and Conditions of Employment of Other Servants for lodging complaints or submitting an appeal pursuant to Article 270 of the Treaty on 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 European Ombudsman must be preceded by the appropriate administrative approaches to the institutions and bodies concerned.