OPEN CALL FOR TENDERS

*concludes with a **Framework service contract in cascade***

Tender Documentation

Cybersecurity Foresight Consultancy Services

ENISA F-KIT-23-T01

Part 1 **Introduction to ENISA**

Part 2 **Terms of Reference**

Part 3 **Tender Specifications**

Annex I	Legal Entity & Financial ID Forms
Annex II	Simplified Financial Statement form
Annex III	Declaration on honour on exclusion criteria and selection criteria
Annex IV(a)	Financial Offer form
Annex V	Draft Framework Service contract
Annex VI	Power of Attorney for Consortium Forms
Annex VII	Sub-Contractors Form
Annex VIII	Administrative ID and Declaration form

e-Submission

*Offers via e-Submission portal **ONLY***

CONTENTS

PART 1 ABOUT ENISA

1.1 INTRODUCTION

The European Union Agency for Cybersecurity (ENISA) was established by the European Parliament and the Council Regulation (EU) No 2019/881 of 17 April 2019 (OJ L 151/15, 07.06.2019). ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow.

1.2 SCOPE

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.

The permanent mandate and enhanced role of the Agency established by the 2019 EU Cybersecurity Act (CSA) and ENISA's new strategy are two milestones that mark an unprecedented and exciting period in the 17 years of the Agency´s life. ENISA aims to build from these two success stories and continue to raise cybersecurity awareness in the EU public fora. In addition, as regards to Article 3 (1c) of the MB decision MB/2020/9 planning, coordinating and implementing communication and outreach activities, the Agency needs to support the necessary activities to fulfil tasks as set out in Art. 21 and 23 of the CSA.

In order to do so the Agency's communications sector supports the implementation of the Agency's Annual Work Programme and has developed a Multi-Annual Communication Strategy and a brand positioning strategy. The strategy lists the steps that the Agency needs to undertake to strengthen its existing communication activities and credibility among its key stakeholders while serving its strategic and policy goals.

1.3 OBJECTIVES

The Agency's objectives are as follows:

- ENISA shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.
- ENISA shall assist the Union institutions, bodies, offices and agencies, as well as Member States, in developing and implementing Union policies related to cybersecurity, including sectoral policies on cybersecurity.
- ENISA shall support capacity-building and preparedness across the Union by assisting the Union institutions, bodies, offices and agencies, as well as Member States and public and private stakeholders, to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities, and to develop skills and competencies in the field of cybersecurity.
- ENISA shall promote cooperation, including information sharing and coordination at Union level, among Member States, Union institutions, bodies, offices and agencies, and relevant private and public stakeholders on matters related to cybersecurity.

- ENISA shall contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats, in particular in the event of cross-border incidents.
- ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation, with a view to increasing the transparency of the cybersecurity of ICT products, ICT services and ICT processes, thereby strengthening trust in the digital internal market and its competitiveness.
- ENISA shall promote a high level of cybersecurity awareness, including cyber-hygiene and cyber-literacy among citizens, organisations and businesses.

2. ADDITIONAL INFORMATION

Further information about ENISA can be obtained on its website: www.enisa.europa.eu.

PART 2 TERMS OF REFERENCE

I. SCOPE OF THIS TENDER

The purpose of this Call for Tenders is for the Agency to acquire the necessary services that will contribute to the ENISA strategic objective SO6: "Foresight on emerging and future cybersecurity challenges". The envisioned services to be provided may include:

- cybersecurity foresight services to ENISA and its communities of stakeholders;
- analysis of future and emerging cybersecurity scenarios;
- analysis of emerging and future cybersecurity challenges and provision of relevant recommendations;
- identification of policy gaps in areas of emerging technologies.
- support the preparation of foresight scenarios on cybersecurity challenges aiming to identify emerging and future cybersecurity research needs;
- analyse trends on emerging technological, political and societal changes with impact in the security of cyberspace that may anticipate future needs of specific research activities;
- prepare wild cards and identify weak signals;

ENISA will use the cascade system to establish framework contracts with multiple economic operators, in order to ensure the management of a fluctuating workload in the areas covered by this call for tenders, while maintaining high quality outputs. A maximum number of three framework contracts in cascade will be awarded.

A more detailed description of the cascade system can be found in Section 17.

Subject of the tender	Maximum budget
Cybersecurity foresight consultancy services	A maximum budget of **€910.000,00 (nine hundred and ten thousand euros)** over the maximum possible period of **4 years**
Last date for dispatch of offers	**13th March 2023 until 18:00 CET**
PLEASE NOTE: *In the case where unforeseen circumstances result in this contract being consumed faster than originally planned, the Agency reserves the right to consider conducting a 'Negotiated procedure without prior publication of a contract notice' with the existing contractor in order to increase the maximum amount stated above by* ***up to 50%.*** *This procedure being fully in accordance with Article 164(4) and Annex I - point 11.1(e) of the EU Financial Regulation (FR)).* *This tender procedure is limited to tenderers which are legally incorporated or which have an incorporated subsidiary in a member state of the European Union/EEA as well as SAA and AA countries[1] . The Agreement on Government*	

[1] Under the Stabilisation and Association Agreements (SAA) economic operators established in FYROM, Albania, Montenegro, Serbia, Bosnia and Herzegovina and Kosovo have been granted access to procurement procedures of the Union institutions, agencies and bodies. Under the Association Agreements with Georgia, Moldova and Ukraine economic operators established in those countries have been granted access to procurement procedures of the Union institutions, agencies and bodies, for all supplies and services with the value equal or above 133.000 EUR, subject to general exceptions.

Procurement (GPA) does not apply to EU Regulatory Agencies and as such, ENISA cannot accept offers from legal entities based in 'third countries'.

IMPORTANT: For entities outside the EU (including UK based entities):

The United Kingdom is now considered a 'third country by the European Union'. ENISA cannot therefore accept submissions from legal entities based in the UK, nor can a UK legal entity be nominated as part of a consortium. Subcontracting of UK (and other third country) entities is allowed. In these cases, any transfer of personal data to third countries shall only take place after prior authorisation of ENISA and shall fully comply with the requirements laid down in Chapter V of Regulation (EU)2018/1725.

Method of submitting tenders: 	***e-Submission portal***	***YES***
	Courier or postal service	*NO*
	By hand	*NO*
	By email	*NO*

1. GENERAL DESCRIPTION OF THE REQUIRED SERVICES

CONTEXT OF THE WORK

The European Union Agency for Cybersecurity (ENISA) strategy[2] clearly sets the goal for Strategic objective 6: "Foresight On Emerging And Future Cybersecurity Challenges" with 2021 marking the start of a new chapter that will enable the Agency to deliver services such as (non-exhaustive list):

- conduct cybersecurity foresight exercises and scenario planning, long-range planning, systematic trend watching and visioning;
- understand emerging trends, gaps and patterns;
- assess emerging challenges and risks and provide relevant recommendations;
- collaborate with stakeholders, decision- and policy-makers on appropriate mitigation strategies;
- identify policy gaps and recommendations in areas related to emerging technologies;
- improve the EU resilience to cybersecurity threats and find solutions to address emerging challenges.
- identify research and innovation needs and priorities addressing emerging cybersecurity challenges and opportunities;
- understand emerging trends and patterns in the technological, societal, economic, regulatory and legal space that may represent an opportunity for EU cybersecurity research and industry.
- conduct foresight exercises (including horizon scanning) to identify scenario, trends, wildcards and week signals to support early detection and assessment of cybersecurity challenges and opportunities for research;
- Provide recommendations on priorities for cybersecurity research and innovation initiatives.

The aforementioned services are within the scope of this Framework Contract.

[2] See https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy

To this end, ENISA has formed a dedicated ad hoc Working Group on Foresight for Emerging and Future Cybersecurity Challenges[3] and in 2021 developed a methodological framework to set the foundations for future foresight exercises concerning cybersecurity[4].

Having expectations about the future provides a certain confidence to actions and decisions in the present. It's impossible to recognize one's ability to shape the future without knowing where to start or where to go. The benefit of undertaking a foresight exercise is identifying future challenges and, consequently, taking anticipated action.

The interpretation of future challenges from the adoption of emerging technologies, ranging from those that are still in their infancy to those close to mainstream adoption, would benefit from the use of foresight methods. Through a structured process enabling dialogue among stakeholders, decision- and policy-makers would be able to define early mitigation strategies that improve the EU resilience to cybersecurity threats and find solutions to address emerging challenges.

ENISA's foresight activities **make use of the 2021 ENISA framework for mapping emerging cybersecurity challenges** and pave the road for future efforts on identifying emerging/future cybersecurity threats, cybersecurity operational priorities, etc. In the coming years, the framework itself might be adapted as part of the Agency's evolution and this adaptation is a potential service to be rendered under this framework contract. In addition, through a structured process that enables dialogue between the community, industry, stakeholders, decision-makers and policy-makers, ENISA will be able to advise its stakeholders on the needs and priorities for cybersecurity research and innovation (CSA Article 11.a) and consequently contribute to the EU's strategic research and innovation agenda (CSA Article 11.b).

ENISA's foresight projects generally involve the definition of a method and processes and its initial use that will help identify and map **strategic long-term analysis, guidance, advice and recommendations on future and emerging cybersecurity threats covering various timespans.** Additionally, a major part of the work involves identifying and collecting information about present and emerging cybersecurity threats, based on the expected technological, societal[5], legal, economic and regulatory impact and associated drivers of change. The goal is **to identify, anticipate and cover future cybersecurity threats, challenges and opportunities that could affect the Union's infrastructure and services, and our ability to keep our society and citizens digitally secure.**

Having identified future and emerging cybersecurity challenges and opportunities, the Agency works on building knowledge to better understand future cybersecurity concerns, identify relevant threats, provide targeted and proportionate recommendations (technical, policy, strategic) to improve the level of cybersecurity across EU and MS. Examples of potential emerging and future cybersecurity topics that have been identified include (list is non-exhaustive):

[3] See https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence/ad-hoc-working-group-on-emerging-and-future-cybersecurity-challenges

[4] See https://www.enisa.europa.eu/publications/foresight-challenges

[5] In particular, societal changes play an important role in technology adoption: firstly, they drive the creation of new products. Secondly, they play an important role on how existing products are being used. In both cases, societal challenges affect technology deployment and security/privacy issues. Societal changes with regard to digitalization are undoubtedly a significant phenomenon in various aspects of our society. Understanding those changes helps identifying behaviour and habits of end users – that is - deriving various usage scenarios. This, in turn, provides important incentives for protection requirements of end-users. The same way with changes in the economy, as the ones introduced by the digital transformation of businesses and organisations, they have unmeasurable impact in the development of our societies.

- Space infrastructure and space exploration related cybersecurity challenges.
- Supply chain technology and use of novel techniques to counter cybersecurity threats.
- Ubiquity of facial recognition and consequent privacy challenges or counter recognition attacks.
- Virtual Reality and Augmented Reality increased popularity and emerging attack surfaces.
- Autonomous and electric transport shift and relevant emerging threats.
- Post quantum computing and cryptography threats.
- Adversarial Artificial Intelligence (mis)use.
- E-government and e-democracy attack surfaces.
- Sustainable technologies' introduction.

STAKEHOLDERS

Beyond the previously mentioned ad hoc working group on Foresight, to help shape and scope the work, ENISA has also established a dedicated ad hoc working groups for specific future and emerging challenges, such as Artificial Intelligence.

Key tasks of the Foresight ad hoc working group include:

- advising ENISA on developing a foresight methodology for cybersecurity long term scenarios;
- advice on interdisciplinary systems & long-term thinking, long-range planning, systematic trend watching, scenario development, and visioning;
- review of related ENISA deliverables;
- advice ENISA stakeholders, decision-makers and policy-makers on emerging opportunities, risk management and appropriate mitigation strategies;
- generally advising ENISA in carrying out its tasks in relation to foresight in cybersecurity.

The ad hoc working group also provides input to ENISA on scenarios and challenges, the interaction with the working group being a core component of ENISA's stakeholder cycle. Furthermore, stakeholder engagement provides the opportunity for ENISA to consult operational actors and to actively listen to suggestions and ideas.

PAST WORK

The Agency has organized a number of workshops and collaborated with private as well as public authorities; as in the case of the **ENISA "Looking into the crystal ball: A report on emerging technologies and security challenges"**[6]. More recently, in 2021 the Agency report titled **"Foresight Challenges"** and in 2022 **the identification of 2030 cybersecurity threats based on Foresight**[7]**,** aimed at highlighting the most relevant foresight methods based on ubiquity or suitability to ENISA's core needs to adequately address future cybersecurity threats and shape a more secure society.

Performed between March and August 2022, the methodology included collaborative exploration based on the analysis of political, economic, social and technological factors (also known as PESTLE analysis), threat identification and threat prioritisation workshops. With the support of the ENISA Foresight Expert

[6] See https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball

[7] See https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

Group, the CSIRTs Network and the EU CyCLONe experts, ENISA brainstormed in a Threat Identification Workshop to find solutions to the emerging challenges in the horizon of 2030.

In 2022, ENISA published a report on cybersecurity research and innovation needs and priorities that examined artificial intelligence, biotechnology, and cryptography. These areas were identified by ENISA stakeholders as some of the most important. Going forward, ENISA intends to conduct a foresight exercise to determine priority areas for each year as a first step in the exploratory process to identify research and innovation needs and priorities.

The study considered the four groups of threat actors, as referred to in the ENISA Threat Landscape report[8], and used the current threat taxonomy dividing threats into high-level categories with a specific focus on intentional threats.

In order to identify threats, experts involved in the project resorted to science fiction prototyping or SFP. SFP consists of stories allowing participants to explore a variety of futures approached by different angles. SFP is based on a future scenario derived from trends and experienced from the point of view of a fictional character.

Also used to identify threats, the threatcasting methodology draws from traditional futures studies and military strategic thinking. The idea was to infer models of future environments using research. The analysis therefore included scenario planning techniques and 5 scenarios were devised:

- Blockchain, deepfakes & cybercrime in a data-rich environment;
- Eco-friendly, sustainable, and interconnected smart cities (non-state actors);
- More data, less control;
- Sustainable energy, automated/short-term workforce;
- Legislation, bias, extinctions & global threats.

Concerning analyses and recommendations for future and emerging challenges, ENISA has undertaken work in several areas including but not limited to Internet of Things (IoT), Industry 4.0, Artificial Intelligence, 5G, Machine Learning, Post-quantum cryptography, autonomous vehicles, smart hospitals, etc. Relevant publications may be found under: https://www.enisa.europa.eu/publications

2. DESCRIPTION OF SERVICES TO BE PROVIDED

The prospective contractor(s) should be able to deliver services according to the scope of the Agency's work and overarching objectives.

The contractor(s) is expected to perform the similar tasks on regular basis for monitoring the future and emerging cybersecurity landscape, conduct foresight exercises and scenario planning, identify possible scenarios of cybersecurity developments and policy gaps, identifying trends and ad hoc whenever need for dedicated foresight exercises is required.

Services are to be delivered according to the highest standards through a framework contract, in an efficient, and timely manner.

[8] See https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

The profiles are described under Section 3.2. while the daily rate for each profile should be filled in Annex IV(a) - Financial Offer form. This form must be fully and duly completed by the tenderer and the provided daily rates should be used as the basis for costing the 'scenario'.

The objectives of the cybersecurity foresight and analysis of emerging and future challenges services may take but are not limited to, the following forms:

S1- **Conduct foresight exercises.** It includes the planning, organisation, execution and analysis of cybersecurity foresight exercises based on the ENISA foresight methodology and other publicly available methodologies. Foresight exercises are participatory of nature, hence organisation and management of working groups of stakeholders, collecting and processing feedback, analysing results and drafting conclusions are expected. The contractor will have to focus the foresight exercise in the context of cybersecurity, but the drivers of change to be analysed include not only technologies, but also political, environmental, social, economy and legal/policy aspects. A multi-disciplinary approach is thus expected to be followed. A typical example includes the 2022 foresight exercise on identifying future threats for 2030. Other potential examples include the development of short-term scenarios for the identification of how threats will evolve in the coming months, especially in the case of operational cybersecurity.

S2- **Identify trends, threats, opportunities and challenges**. The contractor is expected to apply foresight methodologies and techniques to identify cybersecurity trends, threats, opportunities and challenges. By analysing various pools of data and information stemming from example from the ENISA threat landscape, policy observatory, operational priorities, incident reporting, etc. the contractor should identify weak signals and other notions of trends for future and emerging aspects.

There is a need to understand emerging trends in relation to the upcoming threats, as well as communicating horizon scanning results to various stakeholder groups of ENISA. The task involves: evaluating the need for regular horizon scanning exercises in the cybersecurity threat landscape; monitoring of trends that are important in the construction of scenarios, as well as monitoring of horizon scanning activities and possibly running dedicated horizon scanning processes to complement existing activities.

The contractor is expected to produce deliverables/reports based on the aforementioned analysis and its findings and create dashboards and visual infographics to monitor trends over the course of time. The contractor may be requested to conduct such analysis for a specific NIS2 sector or specific communities of reference. In such case, the contractor is expected to report on the anticipated impact of identified trends, threats, opportunities and challenges to the particular sector. Proposals on how to continuously monitor such trends, threats, opportunities and challenges are expected by the contractor. Analytical and drafting skills are requirements for this task.

S3- **Analyse and provide recommendations for future and emerging challenges.** Following the results of foresight exercises and identification of trends, the contractor is expected to analyse the cybersecurity challenges of future and emerging technologies in order to provide targeted recommendations to ENISA stakeholders. A secondary goal is to provide a better understanding of the evolving threat landscape, identify assets, vulnerabilities and threats related to new technologies and provided targeted and proportionate security controls based on existing standards and good practices. Past and recent relevant work of ENISA on IoT, Artificial Intelligence, 5G, Industry 4.0, etc. provides an indication of the expectations with regards to reports and deliverables. The work is expected to deliver reports and other formats of presentation that will analyse the threat landscape concerning future and emerging challenges and technologies. Analytical and drafting skills are requirements for this task.

S4- **Identification of policy gaps concerning emerging and future challenges.** The contractor should be able to conduct foresight exercises and analyse qualitative and quantitative data and information to

identify potential future gaps in the policy landscape concerning emerging and future challenges. Target recommendations on how to address the gaps are also expected. This work is expected to deliver reports and findings in other formats, and to be aligned with the overall foresight findings of the Agency. Analytical and drafting skills are requirements for this task.

S5 - **Identification of research and innovation priorities in cybersecurity.** The contractor(s) should be able to provide services to ENISA contributing to the identification of research and innovation priorities. Targeted foresight exercises (S1) for research and innovation are expected to be conducted by the contractor involving stakeholders, members of the research and innovation community and industry, as well as analysis of publicly available information related to technological and societal changes among others. The expected result should allow ENISA to monitor the future and emerging cybersecurity landscape, conduct foresight exercises and scenario planning, identifying trends, wildcards and weak signals, map research and innovation priorities, identify research and innovation gaps and propose targeted recommendations on potential future topics for research and innovation uptake. ENISA is planning to conduct regular foresight exercises on cybersecurity on emerging cybersecurity challenges and opportunities.

S6 – Identification of early signs of change and validation through further research. The contractor(s) should be able to provide dedicated horizon scanning services for research and innovation (S2) to ENISA, contributing to the identification of early signs of change including wildcards and week signals. Through the organization of horizon scanning exercises, the potential contractor should be able to identify, analyse and describe new trends (Non-obvious or very recently identified trends likely to weigh significantly on future events), new drivers of change (New conditions that will impact how certain social, natural or technological parameters will evolve), weak signals (Apparently small events or novelties that, combined with other existing elements, could lead to significant changes) and discontinuities (Abrupt changes that either stop certain existing phenomena, introduce major changes in their dynamics or generate novel phenomena). The contractor(s) is expected to conduct further research to validate the findings of the exercise.

Outputs:

- **Draft reports**. The contractor should be able to draft reports for any of the above tasks, indicatively it is mentioned for findings, analyses, recommendations for improving cybersecurity, identification of priorities, gap analyses, lessons learnt, recommendations for research and innovation needs and priorities etc.
- **Pilot exercises** e.g. monitoring of trends;
- **Policy Delphis** for the analysis of cybersecurity policy issues.
-
- Targeted **Foresight/Horizon Scanning exercises**. The contractor(s) should be able to organise foresight/horizon scanning exercises depending on ENISA requirements e.g. research and innovation, involving stakeholders, members of the research and innovation community and industry (selection of participants meeting the profile set by the Agency), analysis of publicly available information related to technological and societal changes , preparation of materials, facilitation of the exercise and reporting on the findings.

It should be noted that the list above is non-exhaustive and that the future contractor(s) may be asked by ENISA to provide support in other areas falling within the scope of cybersecurity foresight and analysis of future and emerging cybersecurity challenges activities.

Respecting the contracting procedure in cascade as described under section 17, the first ranked framework Contractor shall be invited to submit their proposal for a specific assignment described by ENISA analytically in each Request for Services in order to conclude a Specific Contract.

Each Request for Services will include in its terms of reference a description of the content of the deliverables to be provided and the indicative timetable for delivery deadlines.

3 SPECIFIC REQUIREMENTS

3.1 PROVISION OF SERVICES - CONTRACT MANAGER

ENISA will designate a contact point to run this contract and it expects the prospective contractor to designate one Contract Manager (and designated backup) to act as the (single) point of contact for all Agency needs.

The Contract manager shall be responsible for the overall management and administration of the framework contract including the organisation of appointment schedules, requests from and communication with ENISA, i.e., invoicing, etc. The nominated contract manager having a minimum of three (3) years of professional experience in managing contracts shall be able to communicate fluently in the English language. The contractor(s) shall provide an e-mail address and phone number to which all communication shall be channelled.

The prospective contractor(s) shall ensure that sufficient provisions are made to ensure all holidays/absences of its staff are adequately covered, in order to ensure continuous provision of services subject to the contract during all regular working days in Greece, from 08:00 to 18:00 during working days (Monday to Friday).

The tenderer shall also include a description of the working method and working arrangements in place. All communication with ENISA will be in English, being the working language of ENISA, and all deliverables must be provided in English.

3.2 EXPERTS PROFILES

The successful tenderers shall provide CVs of experts describing their experience in similar projects and possible certifications if available. The team of experts will be selected depending on their experience with regard to the specific requirements related to each project. The team may comprise of experts of both junior and senior category, being in balance. You are required to provide only the CVs of experts deemed relevant and experienced on the above-mentioned topics. For this call in particular, we expect that you should include **at least** 4 experts; at least 2 ‘Senior Experts’ and at least 2 ‘Junior Experts’ (see below):

3.2.1 JUNIOR EXPERT PROFILE

The **Junior Expert** shall have:

- Completed university studies (Bachelor’s Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering, Future Studies, Foresight, or equivalent;

- At least three (3) years of professional experience and expertise in cybersecurity, foresight, future studies, research, innovation and emerging trends, risk analysis, technology innovation, horizon scanning. Extensive knowledge of cybersecurity principles, information security and analysis of emerging technologies, implementation and support.
- Proven ability to deliver on issues relevant to foresight and future scenarios development to cover future technological and societal challenges that could impact the Union's infrastructure and services, and our ability to keep our society and citizens digitally secure.
- Proven experience in cybersecurity threat identification and analysis.
- Knowledge of innovation methodologies (e.g. TRL, Design thinking).
- Knowledge of cybersecurity strategy and policy at national and/or European level e.g. the Network Information Security Directive and the European Cyber security strategy for the Digital Decade.
- Cybersecurity strategy and policy at national and/or European level e.g. the Network Information Security Directive and the European Cyber security strategy.
- Security practices and knowledge of the regulatory framework e.g. NIS Directive, the GDPR, the EU Telecoms Package, The European Mobility Packages.
- Excellent knowledge of data collection and validation methods including the ability to produce clear and understandable text equipped with graphical elements.
- Very good writing and communication skills;
- Excellent command of the English language (at least level C1 according to the Common European Framework of Reference for Languages (CEFR));
- Excellent project management skills including quality assurance.

Advantageous:

- Proven participation in at least one (1) foresight exercise.
- Proven participation in at least one (1) multistakeholder and multifaceted analysis of emerging cybersecurity challenges.

3.2.2 SENIOR EXPERT PROFILE

The **Senior Expert** shall have:

- Completed university studies (Bachelor's Degree/Level 6 of the European Qualifications Framework (EQF)) attested by a diploma in Computer Science, Computer Engineering, Future Studies, Foresight, or equivalent;
- At least five (5) years of professional experience and expertise in cybersecurity, foresight, future studies, innovation and emerging trends, risk analysis, technology innovation, horizon scanning. Extensive knowledge of cybersecurity principles, information security and analysis of emerging technologies, implementation and support;

- Recognized competence (e.g., technical, political, organisational or a combination thereof) and experience in the area of interdisciplinary and systems & long-term thinking, long-range planning, systematic trend watching, scenario development, and visioning.
- Proven ability to deliver on issues relevant to foresight and future scenarios development to cover future technological and societal challenges that could impact the Union's infrastructure and services, and our ability to keep our society and citizens digitally secure.
- Proven experience in cybersecurity threat identification and analysis.
- Participation in at least one foresight exercise with a published report.
- Contribution to at least one cybersecurity research project with a published report.
- Participation in the innovation cycle of a cybersecurity product.
- Cybersecurity strategy and policy at national and/or European level e.g., the Network Information Security Directive and the European Cyber security strategy.
- Security practices and knowledge of the regulatory framework e.g., NIS Directive, the GDPR, the EU Telecoms Package, The European Mobility Packages.
- Excellent knowledge of EU cybersecurity policies and funding instruments in the context of research and innovation (e.g. Horizon Europe, Digital Europe, ECCC).
- Excellent knowledge of data collection and validation methods including the ability to produce clear and understandable text equipped with graphical elements.
- Good professional experience in relevant information security issues and disciplines (e.g., security policies and controls).
- Policy and regulatory issues related to the resilience of critical infrastructures and services at national and/or European level including activities related to CIIP.
- Very good writing and communication skills;
- Excellent command of the English language (at least level C1 according to the Common European Framework of Reference for Languages (CEFR));
- Excellent project management skills including quality assurance.

Advantageous:

- Proved organisation of at least one (1) foresight exercise.
- Proven organisation of at least one (1) multistakeholder and multifaceted analysis of emerging cybersecurity challenges.
- Proven experience in identification of emerging and future cybersecurity challenges.

4. PLACE OF EXECUTION OF ACTIVITIES AND COMMUNICATION

The execution of the tasks will normally take place at the contractor's own premises. Network based collaborative tools (i.e., videoconferencing) will be used as normal working methods. The contractor, upon invitation, may be required to visit ENISA's premises at Agamemnonos 14 St. Chalandri, 15231, Attiki, for ad hoc meetings. A kick off meeting shall be convened virtually.

5. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

In this section it is outlined how ENISA expects the tenderer to structure its technical offer responding to this tender. In general, ENISA expects the tenderer to explain how the below mentioned requirements will be met.

5.1 GENERAL REQUIREMENTS

The Tenderer shall enclose with their "Technical Offer", all documents and information that will enable its offer to be assessed in terms of quality and of compliance with the specifications above (the technical description).

The Technical Offer shall include the following:

- Presentation of tender proposal;
- Evidence and material demonstrating expertise in the fields covered by this call for tender;
- Management practices, planning and resource allocation to tasks and experts, available to be used in order to meet the Agency's requirements.
- Project management methodology that will be used for projects under this framework contract, explaining how possible projects would be carried out efficiently, timely and effectively;
- The procedure for the provision of experts (e.g., backup solutions etc.);
- In the case of a tender being submitted by a consortium, a description of the input from each of the consortium members and the distribution and interaction of tasks and responsibilities between them;
- A description of sub-contracting arrangements foreseen, if any, with a clear indication of the tasks that will be entrusted to a sub-contractor and the award methods to be used in relation to these tasks. A statement by the tenderer guaranteeing the eligibility of any sub-contractor shall be included as well, in case the subcontractor/s are not known at the moment of the tender submission.

The content of the technical offer is important for the award of the contract and the future execution of any resulting contract. Some guidelines are given above, but attention is also drawn to the award criteria, which define those parts of the technical proposal to which the tenderers should pay particular attention.

The technical proposal should address all matters laid down in the technical specifications as described. Please note that, to ensure equal treatment to all tenderers, it is not possible to modify your offer after the expiry date. Consequently, incompleteness in this section can only result in a negative impact for the evaluation of the award criteria.

The Offer shall **consist of 30 pages maximum**. Pages over the limit will not be considered for evaluation. Any detailed CVs of proposed team members shall be submitted separately or in Annex. The Tenderer is encouraged to provide specific details for each section of the offer; simple repetition of the terms of reference and tender specification will result in a very low technical score.

5.2 SCENARIO

The following scenario must be assessed and a technical description of how you would implement and deliver the final deliverable be provided as part of your technical offer (see section 5.1 above). Your actual estimations of volume of work required in 'person days' per profile and overall project cost shall

then be entered into the appropriate 'scenario' boxes in the Financial Offer form (Annex IV). This scenario refers to a possible situation in accordance with ENISA needs, in order to facilitate the tenderer towards building a reliable and comparable financial offer. The actual projects to be awarded to the successful contractor will have a much more detailed level of technical specifications.

Failure to provide an estimation for the scenario may result in your offer being declared invalid and not further evaluated.

SCENARIO 1

As demonstrated by the recent years, disruptive events can occur suddenly and without warning. In those cases, it is prudent to have a structured process with which to generate possible outcomes for this scenario. The contractor is required to envision possible future scenarios following a large disruptive event and write a preliminary report on these scenarios within max 1 week.

The goal is to provide an overview of the impact of disruptive events and outlook of possible future states in order to support informed decision making.

Please provide methodology and detail the project planning and management of the activities described in this scenario:

- Define scope and analyze event
- Identify Key driving factors and forces, emerging events, possible alternate future states also through stakeholder engagement
- Describe possible future evolution of a cyber security event which had a cross border impact
- Drive the stakeholder validation
- Finalize the report based on the input received.

6. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

The Financial offer must be drawn up using the **Financial Offer form (see Annex IV)**.

In order to be considered a valid offer, it must be duly filled in, dated, stamped, and signed by the authorised person.

Please take special care to enter prices **in all boxes** as described and instructed in the Financial Offer form.

Failure to provide a fully and duly completed form may result in your offer being declared invalid and not being further evaluated.

7. TENDER RESULT AND ESTIMATED CONTRACT VALUES

The result of the evaluation of tenders will be the awarding of a Framework Service Contract. The estimated overall maximum contract value without this being binding for ENISA is **nine hundred and ten thousand Euro (€ 910,000.00)** over a maximum possible period of four (4) years.

It is important to note that the amount stated above applies to **all** framework contracts signed under the 'cascade' system in total and not for each framework contract. There will be a minimum of two and a maximum of three framework contracts signed, if there are a sufficient number of admissible tenderers that meet the award criteria and minimum quality points following the evaluation of offers.

(Please note that in the case where unforeseen circumstances result in this contract being consumed faster than originally planned, the Agency reserves the right to consider conducting a 'Negotiated procedure without prior publication of a contract notice' with the existing contractor in order to increase the maximum amount stated above by up to 50%. This procedure being fully in accordance with Annex I - point 11.1(e) of the EU Financial Regulation (FR)).

8. DATA PROTECTION AND TRANSPARENCY

Processing of personal data in the context of this contract shall comply with the legal framework on data protection, i.e.:

- **Regulation (EU) 2018/1725[9] ('the EDPR')** as concerns personal data processing by the selected contractor, processing data in execution of the contract with ENISA.

The EDPR constitutes the specific data protection legal framework applicable to institutions, bodies, offices and agencies of the European Union, including ENISA, mirroring the GDPR applicable within the Union.

ENISA is the controller under this Regulation and the prospective contractor is the processor. The processor shall act only under the instructions of ENISA. ENISA's terms and conditions concerning procurement contracts are included in Article II.9.2 of the draft contract in Annex V.

- **Regulation (EU) 2016/679[10] (General Data Protection Regulation – 'the GDPR')** as concerns personal data processing carried out by the contractor on its proper behalf as a controller.

Processing of personal data by ENISA as contracting authority:

Information on the processing of personal data by ENISA as contracting authority in charge of the present procurement procedure is available in the Privacy Statement on the ENISA website as well as in Article II.9.1 of the draft contract in Annex IV. In this context, please be informed that ENISA may register your personal data as a tenderer or selected contractors in the Early Detection and Exclusion System (EDES) if you are in one of the situations mentioned in Article 136 of the Financial Regulation. The relevant Privacy Statement is available on the European Commission's website, here: http://ec.europa.eu/budget/explained/management/protecting/protect_en.cfm#BDCE.

Processing of personal data by the selected contractor:

Personal data processing in execution of the contract between ENISA and the selected contractors shall comply with Regulation (EU) 2018/1725 (the EDPR).

The processing of personal data shall happen in accordance with Article 29 of the EDPR. In particular, the selected contractor shall comply with the following:

- to process the personal data only on documented instructions of ENISA, in particular with regard to the purposes of the processing, the categories of data that may be processed, the recipients of the data and the means by which the data subject may exercise its rights;

[9] 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, OJ L 295/39 21.11.2018

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1–88

- to ensure that access to personal data is granted to the extent strictly necessary for the implementation of the contract and to ensure that persons authorised to process the personal data have committed themselves to confidentiality ;
- to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks, in particular the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the personal data, processed or stored;
- not to engage another processor of personal data (i.e. by means of a subcontract), without prior written authorisation of ENISA. Where another processor is engaged for carrying out specific processing activities on the personal data, the same data protection obligations as set out in the contract shall be imposed on the other processor;
- to assist ENISA in the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the EDPR;
- to assist ENISA with its obligations with regard to security of processing, the notification obligations in case of a personal data breach, as well as where applicable cooperation in data protection impact assessments (DPIAs) and prior consultations with the European Data Protection Supervisor (the EDPS)[11], outlined in Art. 33 to 40 of the EDPR ;
- to make available to ENISA all information to demonstrate compliance with the obligations laid down in the EDPR and to allow for and to contribute to audits, including inspections, conducted by ENISA or another auditor mandated by ENISA;
- As concerns the localisation of and access to the personal data, to comply with the following:
    - the personal data shall only be processed and held in data centres within the territory of the European Union and the European Economic Area and will not leave that territory. This includes also any backup centres and location of backup data.;
    - the contractor may not change the location of data processing without the prior written authorisation of ENISA ;
    - The contractor shall inform ENISA in case of any need for transfer of personal data to third countries or international organisations and will perform such transfer only after written authorisation by ENISA. Any transfer of personal data to third countries or international organisations shall fully comply with the requirements laid down in Chapter V of the EDPR ;
    - The contractor shall notify ENISA without delay of any legally binding request for disclosure of the personal data processed on behalf of ENISA made by any national public authority, including an authority from a third country. The contractor may not give such access without the prior written authorisation of ENISA;
        - To contact the Data Protection Officer (DPO) of ENISA, in charge of monitoring data protection compliance, with any questions arising or in case of need for assistance concerning personal data protection dataprotection@enisa.europa.eu,

In addition, **Article II.9.2 of the draft contract** provided in Annex V is applicable.

Confidentiality:

ENISA will disregard general statements that the whole tender or substantial parts of it contain confidential information. Tenderers need to mark clearly the information they consider confidential and

[11] http://www.edps.europa.eu

explain why it may not be disclosed. The EU body reserves the right to make its own assessment of the confidential nature of any information contained in the tender.

Based on the projects assignments, scope, terms of engagement, possibly NDAs may be required to be signed before the projects' initiation

9. MARKING OF SUBMITTED DOCUMENTS

The tenderer SHOULD NOT mark tender documents (for e.g. the header or footer) with any of the following words: RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET. If the tenderer considers that such markings are required, a prior approval from the ENISA Procurement Coordinator should be obtained BEFORE sending the tender documents. The tenderer should be aware that the information sent to ENISA for procurement purposes is handled in accordance with the governing rules for EU Public Procurement and the EU Financial Regulation framework.

10. PRICE

Prices submitted in response to this Tender must be inclusive of all costs involved in the performance of the contract. Prices shall be submitted only in Euro and VAT excluded.

11. PRICE REVISION

The price quoted must be fixed and not subject to revision during the first year of performance of the contract. From the beginning of the second year of performance of the contract, prices may be revised in accordance with Article I.3.3 of the framework contract.

12. COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER

ENISA will not reimburse any costs incurred in the preparation and submission of a Tender. Any such costs must be paid by the Tenderer.

13. PERIOD OF VALIDITY OF THE TENDER

Tenderers must enclose a confirmation that the prices given are valid for six (6) months from the date of submission of the tender.

14. PROTOCOL ON PRIVILEGES & IMMUNITIES OF THE EUROPEAN UNION

ENISA is exempt from all taxes and duties, including value added tax (VAT), pursuant to the provisions of Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Union. Tenderers must therefore give prices, which are exclusive of any taxes and duties and must indicate the amount of VAT separately.

15. PAYMENT ARRANGEMENTS

Payments under the Contract shall be carried out, subject to prior approval of the report accompanying the invoices, listing the services rendered, within 60 days of submission of an invoice accompanying the final report or deliverable based on the conditions set out in the draft contract.

16. CONTRACTUAL DETAILS

A Framework Service Contract will be proposed to the successful candidates. Selection of a candidates and / or signature of the Framework Service Contract imposes no obligation on ENISA to order services.

The contract and its annexes draw up the legal, financial, technical and administrative provisions governing the relations between the Agency and the Contractor during its period of validity.

The tender will conclude, valid as of the date of the last signature, with a one-year Framework Service contract, tacitly renewable up to three times for a maximum of four years.

The Agency reserves the right to end the contract at any time, without any obligation to invoke the reason for it, at one months' notice. The Tenderer's offer must be drafted taking fully into account the provisions of the draft Framework Service contract annexed to this call for tenders (See draft contract, in Annex V).

Execution of the Framework Contracts will be performed via Specific Contracts following the 'Cascade' procedure.

Please note *that the general conditions of our standard framework service contract cannot be modified. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein.* ***It is strongly recommended*** *that you have this draft contract checked and passed by your legal services before committing to submitting an offer.*

17. PROVISION OF SERVICES – CASCADE SYSTEM

At the conclusion of this tender procedure, at least two and up to three tenderers who are top-ranked following the outcome of the evaluation, will be awarded framework contracts.

ENISA sends a 'Request for Services' on a specific subject matter to the first contractor in the cascade, and only in case the contractor does not accept the request for reasons which do not entail terminating the contract, or fails to observe the deadline for submission of an offer, or is in a situation of conflicting interests that may negatively affect the performance of the specific contract, ENISA may place the order with the next contractor in the cascade. The proposal shall only consist of a technical offer and will not require any administrative paperwork or proof of economic stability to be re-submitted.

In general, the following rules shall apply to requests for supply of Services.

(1) For each case, ENISA shall determine the specifications of the Services required, hereinafter referred as project, and the relevant response time. The Contractor shall make its offer in response to ENISA's specifications within this time limit.

(2) When requesting an offer to supply Services, ENISA shall initially address its request to the contractor who has been nominated in first place on the basis of the results of the evaluation of the call

for tenders cited in the Contract. If this first contractor meets the criteria for response time and fulfil the specifications, then it shall be awarded the project in question.

(3) If the first contractor does not meet either of these criteria, it shall be regarded as being unable to supply the Services requested. In this case, ENISA shall then address the same request to the contractor who has been nominated in the second place on the basis of the results of the evaluation of the call for tenders cited in the Contract. If this second contractor is in a position to meet the criteria for response time and specifications, then it shall be awarded the project in question.

(4) If this second contractor is unable to meet either of these criteria, then it shall be considered unable to supply the Services requested. In that event, ENISA shall repeat this process with the contractor who has been nominated in third place.

(5) This process will terminate either with the award of the project in question to one of the contractors who has been nominated, or with the failure to award the project to any contractor. In the event of failure, ENISA may redefine the project or start the procedure again on the same project at a later time.

(6) The inability of the Contractor to supply the Services for a project, requested under the conditions (1) – (5), shall not be considered as such to afford grounds for terminating the Framework Contract, nor shall it affect the order in which the Contractor is to be addressed for subsequent projects.

Except in the case of a conflict of interests, the first contractor must be consulted first. If it arises that the main contractor is unable to satisfy a request, the cascade mechanism may be applied. In this case careful documentation of all communication between the contractors and ENISA is imperative in order to ensure a decision transparent to all parties.

During the cascade mechanism the Request Form specifications may not change (e.g. description of services and/or technical annexes must remain the same).

- The Framework Contractors will be required to respond typically within 3 - 5 working days with a detailed technical proposal, depending on the complexity of the project. This offer will contain all aspects regarding:
    - Technical content relevant to the specific subject matter
    - Experts proposed (*they should be from the pool of experts already included in the contract but alternatives can be proposed in exceptional circumstances which are well documented*)
    - A project plan
    - Proposed duration of consultancy in person-days
    - Cost

ENISA will evaluate the offer received by the closing date for reception of the proposal. A Specific Contract will be concluded according to the abovementioned cascade procedure.

For each Specific Contract the contractor will designate a Project Manager. The Project Manager will be responsible for overall management of the assignment, the timely completion of the activities and the quality and timely delivery of the deliverables.

PART 3 TENDER SPECIFICATIONS

1. INFORMATION ON TENDERING

1.1 CONTRACTUAL CONDITIONS

In drawing up their offer, the tenderer should bear in mind the provisions of the draft contract (Annex V) attached to this invitation to tender particularly those on payments, performance of the contract, confidentiality, and checks and audits. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein. Any limitation, amendment or denial of the terms of contract will lead to automatic exclusion from the procurement procedure.

It is strongly recommended that you have this draft contract checked and passed by your legal representative before committing to submitting an offer.

Before the contract is signed, the Agency may decide to abandon the procurement procedure or cancel the award procedure without the tenderers being entitled to claim any compensation.

1.2 JOINT TENDERS (IF APPLICABLE)

A joint tender is a situation where a tender is submitted by a 'group' of economic operators (consortium). Joint tenders may include subcontractors in addition to the joint tenderers.

Tenders can be submitted by groupings of service providers/suppliers who will not be required to adopt a particular legal form prior to the contract being awarded. However, the Agency will require the grouping:

- Either to have the contract signed by all members (partners) of the grouping. In this case, one of them, as 'Lead Partner', will be responsible for the receipt and processing of payments for members of the grouping, for managing the service administration and for coordination of the contract;
- Or to have the contract signed by the 'Lead Partner' only, who has been duly authorised by the other members to bind each of them (a fully completed 'power of attorney' form for each member of the Group will be attached to the contract according to the template provided by the Agency).

In addition, the composition and constitution of the grouping, and the allocation of the scope of tasks amongst the members, shall not be altered without the prior written consent of the Agency, which can be withheld at its discretion.

In case of a joint offer, each member of the grouping shall provide the following:

- a **Legal Entities form** and a **Power of Attorney of each consortium partner**, must be filled in, signed by (an) authorised representative(s), scanned and uploaded in the corresponding section.

- a **Declaration of honour with respect to the Exclusion Criteria and absence of conflict of interest** must be filled in, signed by (an) authorised representative(s), scanned and uploaded in the corresponding section.

1.3 LIABILITY OF MEMBERS OF A GROUP

Partners in a joint offer assume **joint and several liability** towards the Agency for the performance of the contract as a whole.

Statements, saying for instance:

- That one of the partners of the joint offer will be responsible[12] for only one part of the contract and another one for the rest, or
- That more than one contract should be signed if the joint offer is successful

are thus incompatible with the principle of joint and several liability. The Agency will disregard any such statement contained in a joint offer, and reserves the right to reject such offers without further evaluation, because they do not comply with the tendering specifications.

1.4 SUBCONTRACTING

Subcontracting is permitted in the tender but the contractor will retain full liability towards the Contracting Authority for performance of the contract as a whole.

If the tenderer intends to subcontract part of the service, they shall indicate in their offer which part will be subcontracted and to what extent (% of the total contract value).

Tenderers must ensure that Article II.7 of the contract (Annex V) can be applied to subcontractors.

Tenderers must give an indication of the proportion of the contract that they intend to subcontract.

Tenderers are required to identify all subcontractors.

During contract execution, any change of a subcontractor identified in the tender will be subject to prior written approval of the Contracting Authority.

2. STRUCTURE AND CONTENT OF THE TENDER

2.1 GENERAL

Tenders must be written in **one of the official languages** of the European Union. The working language of ENISA is English.

Tenders must be written in a clear and concise manner, with continuous page numbering. Since tenderers will be judged on the content of their written bids, they must make it clear that they are able to meet the requirements of the specifications/terms of reference.

[12] not to be confused with distribution of tasks among the members of the grouping

2.2 STRUCTURE OF THE TENDER

Based on the ***e-Submission*** environment[13], all tenders must provide information and supporting documentation in two sections:

1) Qualification - data and documentation;

2) Tender offer - data and documentation.

2.3 QUALIFICATION DATA

a) Identification of the Tenderer

The tenderer must fill in all required fields in the qualification section. In case of a joint tender the consortium name has to be provided and an identification of every party in the consortium needs to be added.

The following information should also be provided:

(i) Legal Entities

In order to prove their legal capacity and their status, all tenderers and identified subcontractors must provide a Legal Entity Form with its supporting evidence.

However, the subcontractor(s) shall not be required to fill in or provide those documents when the services represent less than 20% of the overall contract value.

The Legal Entity Form can be generated via the e-Submission application. Alternatively, a standard template in each EU language is available at:

http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal_entities_en.cfm

Tenderers must provide the following information if it has not been included with the Legal Entity Form:

- For **legal persons**, a legible copy of the notice of appointment of the persons authorised to represent the tenderer in dealings with third parties and in legal proceedings, or a copy of the publication of such appointment if the legislation, which applies to the legal entity concerned, requires such publication. Any delegation of this authorisation to another representative not indicated in the official appointment must be evidenced.
- For **natural persons**, where applicable, a proof of registration on a professional or trade register or any other official document showing the registration number.

(ii) Financial identification

The tenderer (or the single point of contact in case of joint tender) must provide a Financial Identification Form and supporting documents. Only one form per offer should be submitted (no form is needed for subcontractors and other joint tenderers). The form is available at:

http://ec.europa.eu/budget/contracts_grants/info_contracts/financial_id/financial_id_en.cfm

[13] *For detailed instructions on how to submit a tender please consult the e-Submission Quick Guide available at: https://webgate.ec.europa.eu/digit/opsys/esubmission/assets/documents/manual/quickGuide_en.pdf*

Remark: Tenderers that are already registered in the Agency's accounting system (i.e. they have already been direct contractors **with ENISA** in the past) must provide the filled in form but are not obliged to provide the supporting evidence.

The form needs to be printed, filled in and then scanned and uploaded in the Qualification section. In case of a joint tender, it has to be uploaded in the ***"Documents"*** section of the Consortium Leader.

(iii) Power of Attorney

In case of a joint tender, an Agreement / Power of Attorney for each partner must be filled in, signed by (an) authorised representative(s), scanned and uploaded. Please choose 'Model A' for an ad hoc grouping or 'Model B' for a legally constituted consortium - see templates in Annex VI (a) and (b)

(iv) Lots interested in *(only in case the tender has multiple lots)*

The tenderer must indicate for which lots the tender is applicable, by ticking the relevant boxes in the section: ***"Interested in the following lots".***

b) Information regarding exclusion and selection criteria:

The tenderer is requested to submit the following documents:

1. Declaration by the Tenderer relating to the exclusion criteria (see 3.1 below)

   The filled-in Declaration form.

   In case of a joint tender, each member of the consortium has to submit a declaration under the respective party name (see template in Annex III)

2. Documents certifying economic and financial capacity (see 3.2.2 below)

   In case of a joint tender, each member of the consortium has to submit the documents under the respective party name.

3. Proof of technical and professional capacity (see 3.2.3 below)

   In case of a joint tender, each member of the consortium has to submit the documents under the respective party name.

If any of the above documents are associated with a specific Lot, please indicate for which Lot it is applicable inside the document AND in the Description field of the attachment *(only in case the tender has multiple lots).*

2.4 TENDER DATA

a) Technical proposal

The technical section is of great importance in the assessment of the bids, the award of the contract and the future execution of any resulting contract.

The technical offer must cover all aspects and tasks required in the technical specification and provide all the information needed to apply the award criteria. Offers deviating from the requirements or not covering all requirements may be excluded based on non-conformity with the tender specifications, and will not be evaluated.

The technical tender needs to be uploaded in the relevant section:

The tenderer selects the "Technical Tender" document from the dropdown box ("Financial Tender or Technical Tender"). The e-Submission application allows attachment of as many documents as necessary.

b) Financial proposal

- All tenders must contain a financial proposal, to be submitted **using the form attached as Annex IV(a).**

The tenderer's attention is drawn to the following points:

- Prices must be quoted in **euro**, including the countries that are not in the euro-zone. As far as the tenderers of those countries are concerned, they cannot change the amount of the bid because of the evolution of the exchange rate. The tenderers choose the exchange rate and assume all risks or opportunities relating to the rate fluctuation.
- **Prices must be fixed amounts**.
- **Estimated travel and daily subsistence allowance expenses must be indicated separately**. *(only if applicable to this procedure)*

  This estimate should be based on Articles I.5 and II.22 of the draft framework contract (Annex V). This estimate will comprise all foreseen travel and will constitute the maximum amount of travel and daily subsistence allowance expenses to be paid for all tasks.
- **Prices must be quoted free of all duties**, taxes and other charges, including VAT, as the European Union is exempt from such charges under Articles 3 and 4 of the Protocol on the privileges and immunities of the European Union. The amount of VAT may be shown separately.
- Prices shall be fixed and not subject to revision during the performance of the contract.

The total price needs to be encoded in the e-Submission application[14].

- In the box labelled ***'Total amount exclusive of taxes'*** – please add the amount Total P_B from your Financial Offer form.
- In the box labelled ***'Total taxes amount'*** – please put zero *(if this is not accepted by system then enter 0,01)*
- In the box labelled ***'Total amount'*** – again simply add the amount Total from your Financial Offer form or the maximum budget assigned for this tender

The completed Financial Offer form(s), MUST ALSO be uploaded in the relevant section:

The tenderer selects the "Financial Tender" document from the dropdown box ("Financial Tender or Technical Tender"). The e-Submission application allows attachment of as many documents as necessary.

[14] In the case of framework contracts, unless otherwise instructed, please add the maximum budget given for this tender

3. ASSESSMENT AND AWARD OF THE CONTRACT

The assessment will be based on each tenderer's bid. All the information will be assessed in light of the criteria set out in these specifications. The procedure for the award of the contract, which will concern only admissible bids, will be carried out in three stages, normally in the order shown below.

The aim of each of these stages is:

1) to check on the basis of the ***exclusion criteria***, whether tenderers can take part in the tendering procedure;
2) to check on the basis of the ***selection criteria***, the legal and regulatory capacity, the technical and professional capacity and economic and financial capacity of each tenderer;
3) to assess on the basis of the ***award criteria*** each bid which has passed the exclusion and selection stages.

Only tenders meeting the requirements of each stage will pass on to the next evaluation stage.

3.1 EXCLUSION CRITERIA

All tenderers shall provide a 'declaration on their honour' (see Annex III), stating that they are not in one of the situations of exclusion listed.

The 'declaration on honour' is also required for identified subcontractors whose intended share of the contract is above 20%.

The 'declaration on honour' has to be duly signed by parties that are not signing the Tender Preparation Report in *e-Submission*.

The successful tenderer shall be asked to provide the actual documents mentioned as supporting evidence in Annex III before signature of the contract and within a deadline given by the contracting authority. This requirement applies to all members of the consortium in case of joint tender.

Remark:

A tenderer may be waived of the obligation to submit the documentary evidence mentioned above if such evidence has already been submitted for the purposes of another procurement procedure launched by ENISA, provided that the documents are ***not more than one-year-old*** starting from their issuing date and that they are still valid. In such a case, the tenderer shall declare on his/her honour that the documentary evidence has already been provided in a previous procurement procedure, specifying the reference of the call for tender for which the documents have been provided, and confirm that no changes in their situation has occurred.

ENISA will also waive the obligation of the tenderer to submit the documentary evidence if it can access it on a national database free of charge.

Each tenderer (and each member of a consortium) shall declare in the relevant field in Annex VII (Administrative Identification form) whether it is a Small or Medium Size Enterprise (SME) in accordance with Commission Recommendation 2003/361/EC[15].

As a general guideline, here is an excerpt from the Recommendation:

"*The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.*"

3.2 SELECTION CRITERIA

The following criteria will be used to select the Tenderers for further evaluation. If the Tender is proposed by a consortium, these criteria apply to the tenderer as a whole (unless otherwise stated)..

Documentary evidence of the Tenderers' claims in respect of the below-mentioned criteria is required.

3.2.1 LEGAL AND REGULATORY CAPACITY

The Tenderer must provide evidence of enrolment (declaration or certificates) in one of the professional or trade registers related to the subject of this tender, in the country of its establishment.

3.2.2 FINANCIAL AND ECONOMIC CAPACITY

Proof of financial and economic standing shall be furnished by the following documents and minimum requirements:

(a) Copy of the financial statements (balance sheets and profit and loss accounts) for the last two (2) financial years for which accounts have been closed, where publication of the accounts is required under the company law of the country in which the economic operator is established. In case of a consortium, each consortium member shall present their financial statements.

If the tenderer is not obliged to publish its accounts under the law of the state in which it is established, a copy of audited accounts for the last two (2) financial years should be presented. In case of a consortium/grouping, audited accounts for each consortium partner shall be presented.

(b) **Complete (also) the attached Annex II 'Simplified Financial Statement',** which summarises your recent financial capacity. Please note that the average turnover for the last two (2) financial years for which accounts have been closed must meet our **minimum annual average turnover** of **€225.000,00 (two hundred and twenty five thousand euro)**:

In case of a consortium/grouping, the annual average turnover for each of the partners shall be presented. The sum of the annual average turnovers of each partner will be taken into account to reach the annual average turnover of **€225.000,00**.

[15] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF

(c) If tenderers will call on the competences of another entity (for example, a parent company), a written undertaking by the said entity certifying that it will make available to the tenderers the resources required to implement the contract.

If for some exceptional reason which the Contracting Authority considers justified, the tenderer is unable to provide the documentary evidence requested above, he may prove his economic and financial capacity by any other means which the Contracting Authority considers appropriate, but only following a formal request for clarification **before** the tender expiry date.

3.2.3 TECHNICAL AND PROFESSIONAL CAPACITY CRITERIA AND EVIDENCE

The Tenderers are required to have sufficient technical and professional capacity to perform the contract. Evidence of the technical and professional capacity of the tenderers shall be furnished on the basis of the following requirements:

Support of the activities of ENISA to acquire necessary services that will contribute to the ENISA strategic objective SO6: "Foresight on emerging and future cybersecurity challenges". The envisioned services to be provided may include:

- cybersecurity foresight services to ENISA and its communities of stakeholders;
- analysis of future and emerging cybersecurity scenarios;
- analysis of emerging and future cybersecurity challenges and provision of relevant recommendations;
- identification of policy gaps in areas of emerging technologies.

Criterion T1: The tenderer must prove experience in conducting cybersecurity foresight exercises; identifying and analysing future and emerging cybersecurity scenarios, trends, threats, opportunities and challenges, reporting and providing recommendations for future and emerging challenges.
Evidence for T1: Reference list (including contact details) of minimum three (3) current and/or past customers to whom the tenderer has supplied the core services, in the past five (5) years; specifying the tenderer's share (at least 50%) in provision of the services and if subcontractors were used for any of the services.

Criterion T2: The tenderer must prove experience in the identification of cybersecurity policy gaps and opportunities concerning emerging and future technologies and reporting.
Evidence for T2: Reference list (including contact details) of minimum three (3) current and/or past customers to whom the tenderer has supplied the core services, in the past five (5) years; specifying the tenderer's share (at least 50%) in provision of the services and if subcontractors were used for any of the services.

Criterion T3: The tenderers must demonstrate the capacity to build, coordinate and manage the team of experts (experiences, skills and competences of the team indicated in Part 2 Terms of Reference - section 3). The team shall be competent to ensure quality of all the expected results and deliverables.
Evidence for T3: The Curricula Vitae (CVs), preferably in a common European format, of the proposed members of the team must be enclosed, showing clearly qualifications and professional experience within the relevant business area with the start and the end date (i.e. from DD.MM.YYYY to DD.MM.YYYY) and the linguistic skills. The form can be downloaded from:
https://europass.cedefop.europa.eu/en/documents/curriculum-vitae/templates-instructions.

The successful tenderers may be requested to provide the diplomas and professional qualifications of the persons responsible for providing the services, and/or any other type of relevant work in the field that is the object of this contract.

3.3 AWARD CRITERIA

3.3.1 QUALITY OF THE OFFER

Once the Tenderer has demonstrated the appropriate capacity to perform the Contract on the grounds of the selection criteria, the offer will be assessed based on the award criteria.

No	Qualitative award criteria		Weighting (max. points)
1.	**Quality of the methodological approach and project management and response to scenario**	Quality of the technical proposal including: • Overall methodology and indicative examples for the provided services; • Approach to project management for services listed in section 2, demonstrating good management of processes, information and time; • Capacity and competence to manage multiple concurring assignments and ensure availability of the services; • Capacity to assign tasks to experts based on their skills; • Comprehensive and effective quality assurance system • Quality of technical proposal for the scenario	40
2.	**Quality Control Measures**	Quality control measures including: • Overall risk management strategy; • Change management strategy; • Management of conflicting requirements (working under pressure).	30

3.	**Internal Organisation**	Organisation of work and resources including: • Overall organisation of the project team and quality of the proposed members of the team in regards with the advantageous elements as outlined in section 3.2[16] • Measures to ensure effective communication among team members and between the contractor and ENISA; • Work plan for implementing the framework contract and expected requests for services.	30
Total Qualitative Points (QP)			**100**

Minimum attainment per criterion and overall

Tenders which do not obtain at least 50% of the maximum score for each award criterion and at least 60% of the overall score for all the criteria will be considered to be of insufficient quality and will not be admitted to the next stage of the evaluation procedure.

The sum of all criteria gives a total of 100 points. The respective weighting between the different awards criteria depends on the nature of the services required and is consequently closely related to the Technical Specifications. The award criteria are thus quantified parameters that the offer should comply with. The qualitative award criteria points will be weighted at 70% in relation to the price.

3.3.2 PRICE OF THE OFFER

The evaluation of Financial Offers is based on the total price (overall total referred in Financial Offer form Annex IV page 3).

The cheapest offer will receive the maximum points and the rest of the candidate's offers will be awarded points in relation to the best offer as follows:

PP = (PC / PB) x 100

where:

PP = Price points

PC = Cheapest bid price received

PB = Bid price being evaluated

[16] The knowledge and experience of the proposed team members as regards the advantageous elements as outlined in section 3.2, would be considered under the award criteria only in the way in which those aspects apply for the purpose of this contract.

Please note: If any price box is left blank by the tenderer then the Financial Offer may be considered to be invalid and will be eliminated from further evaluation.

3.3.3 AWARD OF THE CONTRACT

The contract will be awarded to the offer that is the most cost effective (offers the best value for money) which obtains the highest number of points after the final evaluation, based on the ratio between the **quality criteria (70%) and the price (30%).** The following formula will be used:

$$TWP = (Q_P \times 0.7) + (P_P \times 0.3)$$

where;

Q_P = Qualitative points
P_P = Price points
TWP = Total weighted points score

In case the successful tenderer is unable to sign the contract for any reason, the Contracting Authority reserves the right to award the contract to other tenderers as per the ranking order established following the evaluation procedure.

4. TENDER OPENING

The public opening of received tenders will take place online on **14th March 2023 at 09:30 CET Central European Time**.

A maximum of one legal representative per participating tenderer may attend the opening session. Tenderers shall inform the Agency in writing of their intention to attend, by email to procurement@enisa.europa.eu **at least 2 working days** prior to the opening session.

Alternatively, please note *that all tenderers may simply request a copy of the Opening Report to be sent to them by email after the conclusion of the Opening Session procedure.*

5. OTHER CONDITIONS

5.1 VALIDITY

Period of validity of the Tender: 90 days from the closing date stated in Invitation to Tender. The successful Tenderer must maintain its Offer for a further 120 days from the notification of the award.

5.2 LOTS

This tender is not divided into lots.

5.3 ADDITIONAL PROVISIONS

- Changes to tenders will be accepted only if they are received on or before the final date and time set for the receipt of tenders.
- Expenses incurred in respect of the preparation and presentation of tenders cannot be refunded.
- No information of any kind will be given on the state of progress with regard to the evaluation of tenders.
- All documents submitted by Tenderers will become the property of ENISA and will be treated as confidential.

5.4 NO OBLIGATION TO AWARD THE CONTRACT

Initiation of a tendering procedure imposes no obligation on the Contracting Authority to award the contract. Should the invitation to tender cover several items or lots, the Contracting Authority reserves the right to award a contract for only some of them. The Contracting Authority shall not be liable for any compensation with respect to Tenderers whose tenders have not been accepted. Nor shall it be so liable if it decides not to award the contract.

6. SPECIFIC INFORMATION

6.1 TIMETABLE

The timetable for this tender and the resulting contracts is as follows:

Title: "**Cybersecurity foresight consultancy services"**

ENISA F-KIT-23-T01

Summary timetable comments

Launch of tender: - Contract notice to the Official Journal of the European Union (OJEU) - Uploaded to e-Tendering website - Uploaded to ENISA website	3rd February 2023	
Deadline for request of information to ENISA	6th March 2023	
Last date on which clarifications are issued by ENISA	8th March 2023	
Deadline for **electronic reception** of offers via ***e-Submission***	**13th March 2023**	**18:00 CET** Central European Time
Opening of offers	14th March 2023	**09:30 CET** Central European Time
Date for evaluation of offers	TBA	
Notification of award to the selected candidate + 10 day standstill period commences	TBA	
Contract signature	Mid April 2023	Estimated