

## **OPEN CALL FOR TENDERS**

*concludes with a **single Framework service contract***

### **Tender Documentation**

## **Supporting analysis of cybersecurity investments and business resilience**

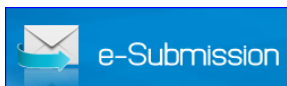
**ENISA F-PDI-22-T37**

**Part 1      Introduction to ENISA**

**Part 2      Terms of Reference**

**Part 3      Tender Specifications**

Annex A	SCENARIO – ‘NIS Investments 2023’
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	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



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

## CONTENTS

<b>PART 1 ABOUT ENISA .....</b>	<b>4</b>
1.1 Introduction .....	4
1.2 Scope.....	4
1.3 Objectives .....	4
2. Additional Information .....	5
<b>PART 2 TERMS OF REFERENCE .....</b>	<b>6</b>
<b>I. SCOPE OF THIS TENDER.....</b>	<b>6</b>
1. BACKGROUND INFORMATION AND OBJECTIVES.....	7
2. PROJECT PROPOSED FOR 2023 .....	8
3. AREAS OF EXPERTISE .....	8
4. DESCRIPTION OF TASKS & SERVICES TO BE PROVIDED .....	9
5. POOL OF EXPERTS AND EXPERT PROFILES .....	10
5.1 Junior Expert profile .....	10
5.2 Senior Expert profile .....	11
6. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER .....	11
7. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER.....	13
8. TENDER RESULT AND ESTIMATED CONTRACT VALUES .....	14
9. DATA PROTECTION AND TRANSPARENCY .....	14
10. OWNERSHIP, INTELLECTUAL PROPERTY RIGHTS, USE OF RESULTS.....	16
11. MARKING OF SUBMITTED DOCUMENTS.....	17
12. PRICE .....	17
13. PRICE REVISION .....	17
14. COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER .....	17
15. PERIOD OF VALIDITY OF THE TENDER .....	17
16. PROTOCOL ON PRIVILEGES & IMMUNITIES OF THE EUROPEAN UNION .....	17
17. PAYMENT ARRANGEMENTS.....	17
18. CONTRACTUAL DETAILS .....	17
<b>PART 3 TENDER SPECIFICATIONS .....</b>	<b>19</b>
<b>1. INFORMATION ON TENDERING .....</b>	<b>19</b>
1.1 Contractual conditions .....	19

1.2	Joint Tenders (if applicable) .....	19
1.3	Liability of members of a group .....	20
1.4	Subcontracting.....	20
<b>2.</b>	<b>STRUCTURE AND CONTENT OF THE TENDER.....</b>	<b>20</b>
2.1	General .....	20
2.2	Structure of the tender .....	20
2.3	Qualification data .....	21
<b>3.</b>	<b>ASSESSMENT AND AWARD OF THE CONTRACT .....</b>	<b>23</b>
3.1	EXCLUSION CRITERIA .....	24
3.2	SELECTION CRITERIA .....	25
3.3	AWARD CRITERIA .....	27
<b>4.</b>	<b>TENDER OPENING .....</b>	<b>29</b>
<b>5.</b>	<b>OTHER CONDITIONS .....</b>	<b>29</b>
5.1	Validity .....	29
5.2	Lots .....	29
5.3	Additional Provisions .....	29
5.4	No obligation to award the contract .....	29
<b>6.</b>	<b>SPECIFIC INFORMATION .....</b>	<b>30</b>
6.1	Timetable .....	30

## 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](http://www.enisa.europa.eu).

## PART 2 TERMS OF REFERENCE

### I. SCOPE OF THIS TENDER

The purpose of this Call for Tenders is to provide support for ENISA's work in assessing cybersecurity investments and business resilience in the private and public sector with a focus on the respective impact of cybersecurity policy, throughout the years 2023 - 2026. ENISA envisages various projects per year in this area, on specific topics such as NIS investments, market trends, economics of cybersecurity, cost of cybersecurity incidents, development of a terminology/methodology for cybersecurity investments etc.


By means of this Call for Tenders ENISA seeks to contract the services of a service provider, which can provide support in the field of cybersecurity investments and business resilience. The successful bidder should be able to demonstrate significant experience and skills in this field, with emphasis on the aspects dealt with in the annual ENISA Work Programme (which is described below).

Subject of the tender	Maximum budget
Supporting analysis of cybersecurity investments and business resilience	A maximum budget of <b>€1.200.000,00</b> <b>(one million, two hundred thousand euro)</b> over the maximum possible period of <b>4 years</b>
Last date for <u>dispatch</u> of offers	<b>3<sup>rd</sup> November 2022 until 18:00 CET</b>

**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)).*

**PLEASE NOTE:** *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 countries<sup>1</sup>. The Agreement on Government 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.*

<b>Method of submitting tenders:</b>  	<b>e-Submission portal</b> <i>Courier or postal service</i> <i>By hand</i> <i>By email</i>	<b>YES</b> <b>NO</b> <b>NO</b> <b>NO</b>
---	---	---

<sup>1</sup> 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.

## 1. BACKGROUND INFORMATION AND OBJECTIVES

Business drivers resulting in digital transformation across sectors of the economy have brought cybersecurity at the forefront for many organisations. This trend has been enhanced by the continuous development of the relevant EU Regulatory and Policy Framework with the introduction of the Network and Information Security (NIS) Directive<sup>2</sup>, the EU Cybersecurity Act<sup>3</sup> and the Digital Single Market Strategy<sup>4</sup> among other initiatives.

In 2020<sup>5</sup> and 2021<sup>6</sup>, ENISA published the first NIS Investments reports with the aim of providing insights into the cybersecurity budgets of Operators of Essential Services (OES) and Digital Service Providers (DSP) and how the NIS Directive has influenced these budgets. This has kickstarted the creation of a historical dataset for certain data points of particular interest, such as % of IT budgets spent on information security that will be monitored in future years to assess how cybersecurity investments evolve in the EU. In addition, a number of the data points collected through this project will feed into the EU Cybersecurity Index currently being developed by ENISA. The EU Cybersecurity Index is comprised of a set of quantitative and qualitative indicators that aim at assessing the level of cybersecurity across Member States and the across the EU as a whole. In this respect, the areas covered by the NIS Investments reports and the corresponding datasets will provide a structured input to the EU Cybersecurity Index.

The NIS Investments report is developing into a regular product that will allow the collection of this data on an annual basis, while also enabling ENISA to collect additional data on selected topics through the survey of private and public sector entities. This data will be used by the Cybersecurity Policy Observatory (CSPO) function established within ENISA to support evidence-based policy making. Within the context of the CSPO, ENISA intends to eventually develop an internal knowledge base where all data collected by this project will be stored. While the development of the knowledge base is not in scope of this Framework Contract, tenderers are encouraged to take it into consideration in their offers, e.g. in relation to making raw data available, applying quality controls to ensure data consistency across different years etc.

In the future, ENISA may look to conduct surveys and publish reports that collect data on the impact of other upcoming legislative instruments on entities falling within their scope, such as the NIS2 Directive, the Cyber Resilience Act (CRA)<sup>7</sup>, the Digital Operational Resilience Act (DORA)<sup>8</sup> etc. Data collected from entities falling in scope of these upcoming legislative instruments will support the assessment of the

---

<sup>2</sup> [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC)

<sup>3</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN>

<sup>4</sup> <https://ec.europa.eu/digital-single-market/en>

<sup>5</sup> <https://www.enisa.europa.eu/publications/nis-investments>

<sup>6</sup> <https://www.enisa.europa.eu/publications/nis-investments-2021>

<sup>7</sup> [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en)

<sup>8</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595>

effectiveness of these legislative instruments in terms of e.g. increasing cybersecurity investments or improving business resilience.

In order to support the above, ENISA is looking to contract services that will support:

- (a) the collection and processing of data on cybersecurity investments and operational resilience of private and public sector entities,
- (b) the collection and processing of data on other topics of interest (e.g. cost of incidents, supply chain aspects etc.) with a focus on providing evidence for policy decisions
- (c) the assessment of the impact of policy on cybersecurity investments and business resilience in the EU
- (d) the identification of market tendencies and large expected shifts, including the identification of tendencies that drive strategy and investments
- (e) the identification of trends on cybersecurity, including how operators organise their cybersecurity, resource/skills gaps and forecasts and market demand/supply side evolution
- (f) the development of insights in any other issue relevant to the economics of cybersecurity
- (g) the development of methodologies, taxonomies and terminologies for collecting data on and understanding the impact of cybersecurity investments

Tenderers are expected to explain their approach and method in relation to data and analyses carried out.

It is important to underline that ENISA is an internal market Agency within the EU, therefore the interest in relation to this study concerns aspects related to considerations affecting the internal market; this for instance would exclude aspects related to policy on defence. ENISA intends to use this data in relation to policy areas it assists with.

## 2. PROJECT PROPOSED FOR 2023

At least one project is foreseen under this framework contract for 2023:

- NIS Investments Report 2023

Details on the project will be shared with the successful tenderer in Q1 2023.

## 3. AREAS OF EXPERTISE

Tenderers are expected to have expertise and knowledge on the following topics.

- Economics and the market in relation to cybersecurity, technology and innovation;
- Impact of policies on affected organisations as regards cybersecurity investments and resilience
- Collection of data from operators; in the interest of time, **ideally the tenderer will have established procedures to collect relevant datasets independently of this framework contract** and possibly have readily available access to data to support the analyses;

- Organisation of cybersecurity in operators across different sectors/industries
- Methodology in social sciences, quantitative, qualitative and mixed methods;
- Analysing data and producing key findings from large datasets – statistical analyses;
- Survey methods to collect quantitative and qualitative economic/market data;
- Knowledge and experience in the field of cybersecurity, technology and innovation;
- Excellent understanding of the cybersecurity market in terms of products, services etc.;
- Excellent knowledge of data collection and validation methods including the ability to draft clearly and accompany text with suitable graphics and visual enhancements;
- Familiarity and experience with the tasks of ENISA;
- Policy and regulatory issues related to the development of policies in the area of cybersecurity, technology and innovation;
- Policy and decision-making / drafting of relevant recommendations in relation to the analysis carried out.

#### 4. DESCRIPTION OF TASKS & SERVICES TO BE PROVIDED

Against the background of ENISA leading this activity, the prospective contractor is expected to carry out a range of tasks and services under the guidance and subject to approval by the Agency. Throughout the period of delivering the said services, ENISA will provide feedback and interact with the prospective contractor. ENISA may provide such guidance acting on its own or in combination with the European Commission and/or duly appointed external experts as appropriate.

In this vein, the objectives of the support services related to studies on cybersecurity investments and business resilience may take but are not limited to, the following forms:

- Collect relevant data on cybersecurity investments and business resilience and support ENISA in the analysis of this data in order to produce key findings; this may involve consolidating data from large existing datasets that the contractor can make available to support a specific project under this framework contract. Relevant data sets, analyses and findings will be submitted to ENISA in draft format;
- Conduct large scale surveys to collect data directly from EU operators, primarily focusing on sectors covered by the NIS Directive
- Under ENISA guidance, carry out analyses based on qualitative and quantitative data, as well use mixed methods as appropriate;
- Carry out a desk research on the topics mentioned above; relevant existing literature, research outputs, policy instruments, legislation;
- Produce graphics and visual enhancements (charts, infographics, slides etc.) to present data as well as analysis;
- Under ENISA guidance perform interviews with designated stakeholders for data collection and/or analysis (e.g. planning, design, implementing, drafting minutes, etc.);
- Under ENISA guidance collect input (initial phase) and feedback (review phase) from related stakeholders for the studies and reports mentioned above. This involves the setting up of online

tools and/or platforms for surveys, questionnaires, polls, etc. based on the content and the requirements set by ENISA on the topics mentioned above;

- Under ENISA guidance support the development of terminologies, taxonomies and methodologies to be used for the assessment of cybersecurity investments and the identification of good practices and benchmarks
- Process the results from interviews, surveys and questionnaires. This may include extraction of statistical values, design of infographics, compilation of summary reports/slides, etc.;
- Support ENISA in the drafting of reports based on collected data and information collected via interviews, surveys or desk research. Support activities in this category may include proofreading, editorial work, substantiating findings by correlating to stocktaking, etc.

The list of tasks connected to the provision of consultancy services is indicative. The successful tenderer may be required to carry out any additional service in support of the above-mentioned objectives in order to ensure efficient and effective delivery of quality material and contribute to meeting the ENISA Work Programme objectives.

Some travelling within the EU may be deemed necessary for example to meet with stakeholders and/or attend relevant meetings. Any required travelling will be clearly specified in the requests for offers under this framework contract.

## 5. POOL OF EXPERTS AND EXPERT PROFILES

The successful tenderer shall have a pool of experts available for individual assignments/tasks. The experts for individual assignments will be selected depending on their availability and experience with regard to the specific requirements related to each project. The pool shall comprise experts of both junior and senior category. 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):

---

### 5.1 JUNIOR EXPERT PROFILE

The **Junior Expert** shall have:

- Minimum 2 years of professional experience in collecting and/or analysing investment, market or operational data and producing key findings from large datasets;
- Minimum 2 years of prior experience (academic or professional) with investment, market or operational data collection and validation methods including the ability to produce clear and understandable text equipped with graphical elements.;
- Social sciences methods.
- Very good drafting skills and ability to draft technical reports;
- Excellent communication and presentation skills;
- Proficient in both written and spoken English;

Advantageous:

- Knowledge of the EU and MS legal framework on cybersecurity on concerning industry and market aspects of cybersecurity;
- Knowledge and experience in the field of cybersecurity;
- Familiarity and experience with the tasks performed by ENISA.

---

## 5.2 SENIOR EXPERT PROFILE

The **Senior Expert** shall have:

- Minimum 5 years of professional experience in collecting and/or analysing investment, market or operational data and producing key findings from large datasets;
- Minimum 5 years of prior experience (academic or professional) with investment, market or operational data collection and validation methods including the ability to produce clear and understandable text equipped with graphical elements;
- Minimum 5 years of prior experience with investment, market or operational studies specifically in the cybersecurity domain and an overall strong understanding of the cybersecurity market demand and supply side;
- Social sciences methods.
- Excellent project management skills including quality assurance and risk management and experience in realising international projects;
- Excellent drafting skills and ability to draft technical reports.
- Excellent communication and presentation skills.
- Proficient in both written and spoken English

Advantageous:

- Knowledge of the EU and MS legal framework on cybersecurity on concerning industry and market aspects of cybersecurity;
- Knowledge and experience in the field of cybersecurity;
- Policy and regulatory issues related to the resilience of critical infrastructures and services at national and/or European level including activities related to CIIP and National Cybersecurity Strategies;
- Familiarity and experience with the tasks performed by ENISA.

## 6. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

---

### 6.1 STRUCTURE OF THE TECHNICAL OFFER

The Tenderer should submit a **Technical Offer** containing relevant documents and information which enables ENISA to assess its quality and compliance with the specifications above (the technical description).

The technical offer shall be structured as follows:

- **Section 1: Methodological approach and Quality Assurance (30% of total score)**
  - **Methodological approach** for the delivery of the indicative tasks.
  - **Methodology and resources for collecting investment and operational data.** The tenderer is encouraged to indicate relevant data that are already available or are collected on a regular basis, details on the methodology for collecting such data and any other/external sources used to obtain missing data to support the relevant analyses.
  - **Conducting large-scale surveys.** Tenderers should present their approach regarding conducting large-scale surveys covering operators in different sectors, with a focus on operators in the sectors covered by the NIS Directive.
  - **Handover of raw data.** It is ENISA's intent to develop an internal knowledge base for the data collected through this framework contract. Tenderers should explain how they will ensure handover of raw data to ENISA to be imported in the knowledge base.
  - The approach and **methodology for the Quality Assurance of data & services** with specific description of quality control of data itself, especially how the data acquired from sub-contractors will be validated and verified.
- **Section 2: Organisation of the work and resources (20% of total score)**
  - Description of relevant **roles/responsibilities** within the proposed framework contract management team
  - Description of **tasks/activities** to be undertaken by each team member and foreseen allocation of resources to the global management of the framework contract.
  - 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 quality assurance methods to be used in relation to these tasks.
- **Section 3: Project Management (20% of total score)**
  - The approach and methodology for the **project management of the specific projects.**
  - General approach to communication and deliverables quality control, including provisions for proof reading of deliverables.
  - Provisions for **continuity of service** in case of absence of a member of a project team.
  - The foreseen **contract/project risks** and how are going to be mitigated.
- **Section 4: Project scenario – “NIS Investments 2023”. (30% of total score)**
  - As per Annex A - Scenario – ‘NIS Investments 2023’

The Technical offer shall consist of **25 pages maximum**. Pages over the limit will not be considered for evaluation. The detailed CVs of the proposed experts for Senior and Junior profiles are not considered part of this page limit. These can be submitted separately or in Annex.

**\*\*Please note** that your technical description for the **Scenario** (see Section 6.2 below) is **also included** in the 25 page maximum limit.

The Tenderer is encouraged to provide specific details for each section of the offer; simply repeating the tender requirements will result in a low score.

In addition to the above the tenderer must provide the information concerning subcontracting as requested in Part 3; section 1.4.

## 6.2 SCENARIO - NIS INVESTMENTS 2023

The objective of this project (see *Annex A Scenario - NIS Investments 2023*) is to support the drafting of a follow-up report consolidating a representative sample of data related to NIS investments by private sector operators in the EU in order to allow for a comprehensive analysis of how the relevant NIS budgets have evolved and what the spending priorities are. The report is intended to serve as a continuation of the previous ENISA reports on NIS investments.

The project has the following objectives:

- Maintain the annual collection of key NIS investments data to develop a historical dataset through a fixed part of the questionnaire (i.e. same set of questions as last year)
- Offer additional granularity in certain types of data (e.g. identify correlations/links between investments and operational capabilities or identify emerging investment priorities)
- Offer insights into operational capabilities of OES/DSP in the EU.

The actual start date for this planned project is estimated around the end of February 2023, and the foreseen project duration is 30 weeks.

The maximum estimated budget assigned for this project is **two hundred and seventy thousand Euros (€270,000.00)**, however this does not mean your scenario budget shall necessarily meet this figure. You are free to propose an amount which is supported with a sound technical offer which fully meets the minimum technical requirements as detailed in 'Annex A - Scenario - NIS Investments 2023'.

The breakdown of costs shall be based on using the 'profiles' in Section 5 above and the daily rates you provide in Part 1 of the Financial Offer form (Annex IV). The actual Scenario costs shall be inserted in Part 2 of the Financial Offer form.

**PLEASE NOTE:** We estimate that, based on the volume and complexity of the required services, a reasonably priced offer will be between **€220.000 and (not higher than) €270.000** - any lower offer may be considered to be abnormally low with the possibility to be declared invalid.

## 7. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

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

Prices/rates must be quoted in **EURO** and include all expenses necessary to perform the contract.

These prices must be a flat rate and include all administrative costs, with the exception of reimbursable costs in relation to travel and overnight stays away from your principal place of business if requested as

part of the subsequent ‘Requests for offers’ under the framework contract’. These costs will be typically reimbursed as follows:

Travel by air will be reimbursed based on return economy tickets. Travel by train or coach will be reimbursed on the basis of a second class ticket. These approximate costs will be provided as part of the contractor’s offer following a ‘Request for offer’ by ENISA.

Any costs incurred during approved business trips such as travel costs and subsistence allowances for overnight stays will be reimbursed based on the *per diem* rates published by the European Commission for the actual dates of the trip. *Per diems* cover accommodation, meals, local travel at the place of the meeting and sundry expenses. Please, refer to the following link for actual rates of reimbursement:

[http://eeas.europa.eu/jobs/docs/20140108/list\\_per\\_diem\\_en.pdf](http://eeas.europa.eu/jobs/docs/20140108/list_per_diem_en.pdf)

Any other costs which may be necessarily incurred will be reimbursed as appropriate, following prior agreement between both ENISA and the contractor, in accordance with the special provisions which will be defined in each Specific Contract.

## 8. TENDER RESULT AND ESTIMATED CONTRACT VALUES

The estimated overall maximum contract value without this being binding for ENISA is **one million and two hundred thousand Euros (€ 1,200,000.00)** over a maximum possible period of 4 years.

*(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 Article 164(4) and Annex I - point 11.1(e) of the EU Financial Regulation (FR)).*

## 9. 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<sup>9</sup> (‘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<sup>10</sup> (General Data Protection Regulation – ‘the GDPR’)** as concerns personal data processing carried out by the contractor on its proper behalf as a controller.

<sup>9</sup> 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

<sup>10</sup> 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

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](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;
- to abide in particular by ENISA's data protection policies as regards the confidentiality of electronic communications (Section 3 EDPR) and the processing of personal data in web services;
- 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)<sup>11</sup>, 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:

---

<sup>11</sup> <http://www.edps.europa.eu>

- 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](mailto: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 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.

## 10. OWNERSHIP, INTELLECTUAL PROPERTY RIGHTS, USE OF RESULTS

As regards any product or delivery commissioned by ENISA and developed by the contractor in the context of the contract resulting from this call for tenders, as well as source codes of IT applications and models developed for ENISA, the intellectual property rights will be owned by ENISA only in its capacity as financial source of the contract. The contractor cannot file a trademark; patent, copyright or other IPR protection scheme in relation to any of the results or rights obtained by ENISA in performance of the contract, unless the contractor requests the ENISA ex-ante authorisation and obtains from ENISA a written consent in this regard.

ENISA does not acquire ownership or any license of pre-existing rights not incorporated in the deliverables. The full ownership is limited to the deliverables, which might include licensed pre-existing rights on excerpts, parts, texts etc., if fully or partially incorporated in the final deliverables.

The draft contract in Annex IV contains further provisions on ownership of intellectual property rights. All quotations or information the tenderer provides in the technical and financial offer for this tender, which originates from other sources to which third parties may claim rights, have to be clearly marked in the offer in a way allowing easy identification (source publications, including date & place, creator, number, full title etc.). The tenderer shall take account of the above specification on ownership and copyrights in their technical and financial offer.

## **11. 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.

## **12. 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.

## **13. 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.

## **14. 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.

## **15. 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.

## **16. 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.

## **17. 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.

## **18. CONTRACTUAL DETAILS**

A Framework Service Contract will be proposed to the successful tenderer. Selection of a tenderer 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).

***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.***

## 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<sup>12</sup> 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.

### 2.2 STRUCTURE OF THE TENDER

Based on the **e-Submission** environment<sup>13</sup>, all tenders must provide information and supporting documentation in two sections:

<sup>12</sup> not to be confused with distribution of tasks among the members of the grouping

<sup>13</sup> 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](https://webgate.ec.europa.eu/digit/opsys/esubmission/assets/documents/manual/quickGuide_en.pdf)

- 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](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](http://ec.europa.eu/budget/contracts_grants/info_contracts/financial_id/financial_id_en.cfm)

**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.**

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<sup>14</sup>.

- In the box labelled '**Total amount exclusive of taxes**' – please add the amount Total P<sub>B</sub> 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.

## 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:

<sup>14</sup> In the case of framework contracts, unless otherwise instructed, please add the maximum budget given for this tender

- 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 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

Tenders will be rejected if they do not comply with applicable obligations under environmental, social and labour law established by Union law, national law and collective agreements, or by the international environmental, social and labour law provisions listed in Annex X to Directive 2014/24/EU and compliance with data protection obligations resulting from Regulation (EU) 2016/679 and Regulation (EU) 2018/1725<sup>15</sup>.

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 VIII (Administrative Identification form) whether it is a Small or Medium Size Enterprise (SME) in accordance with Commission Recommendation 2003/361/EC<sup>15</sup>.

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

---

<sup>15</sup> 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>

*“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 must be fulfilled by each partner (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 €300.000,00 (three 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 **€300.000,00**.

- (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:

#### a) Criteria relating to tenderers

Tenderers (in case of a joint tender the combined capacity of all tenderers and identified subcontractors) must comply with the following criteria:

- The tenderer must prove its experience in the field of investment/market studies with at least two (2) projects/deliverables delivered in this field in the last three years, **at least one (1)** of them covering the NIS/cybersecurity market and each with a **minimum value of € 50,000.00** and **at least one (1)** involving the collection and treatment of data from a **minimum of 300 private or public sector organisations/operators**.
- The tenderer must prove experience of working and drafting reports in the English language with at least three (3) projects delivered in this field in the last five years, showing the necessary language coverage.
- The tenderer must prove its experience of working in EU countries with at least 2 projects delivered in the last three years.
- The tenderer must prove experience in one or more of the following as deemed relevant to the area of expertise the subject of this tender; market/economic data collection, survey techniques, statistical analyses and drafting reports and recommendations.

Please note that your list of previous projects in the fields of expertise mentioned above can be from a wide cross-section of organisations including private industry, commercial enterprises and academia as well as with public or governmental organisations.

#### b) Criteria relating to the team delivering the service:

The team delivering the service should include, as a minimum, the following profiles:

- **Junior Expert profiles** As per minimum requirements listed in Part 2 section 5.1
- **Senior Expert profiles** As per minimum requirements listed in Part 2 section 5.2

#### c) Evidence:

The following evidence should be provided to fulfil the above criteria:

- Details of the structure of the organisation
- List of list of all related projects and activities that the contractor has undertaken in the past five years, particularly in relation to the collection and analysis of cybersecurity market data, with sums, dates and recipients, public or private.
- The educational and professional qualifications of the experts who will provide the services for this tender (CVs), including the management staff. Each CV provided should indicate their intended function in the delivery of the service.

### 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.	<b>Methodological approach and Quality Assurance</b>	This criterion assesses the suitability and strength of the proposal as measured against the requirements of the illustrative tasks in terms of the technical content and the degree to which the methodology is suited to the needs set out by ENISA. Particular emphasis will be placed on the <b>tenderers' approach to collecting the relevant data</b> and on the <b>tenderers' approach to quality assurance for data collected via surveys</b> .	30
2.	<b>Organisation of the work and resources</b>	This criterion will assess how the roles and responsibilities of the proposed team and of the economic operators (in case of joint tenders, including subcontractors if applicable) will be distributed. It also assesses the global allocation of time and resources to the global management of the framework contract.	20
3.	<b>Project management</b>	This criterion will assess the project management approach for the specific contracts the language quality check, and continuity of the service in case of absence of a member of the team	20
4	<b>Project Scenario</b>	Compliance with the technical requirements (Annex A). Quality of the proposal and accuracy of the description to provide the requested services.	30
<b>Total Qualitative Points (QP)</b>			<b>100</b>

#### Minimum attainment per criterion

Offers scoring less than 50% for any criterion will be deemed to be of insufficient quality and eliminated from further consideration.

#### Minimum attainment overall

Offers scoring less than **60%** after the quality evaluation process will be considered to be of insufficient quality and eliminated from the following phase.

The sum of all criteria gives a total of 100 points. The respective weighting between the different award criteria depends on the nature of the services required and is consequently closely related to the terms of reference. 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 Financial Offer form (Annex IV) contains two Parts:

#### Part 1: General Consultancy fees

Consists of two (2) price boxes, which shall be completed with a daily rate by the tenderer.

$P_s$  and  $P_J$  will then be used in the price formula as shown below

**Please note:** If any of the price boxes are left blank by the tenderer then the Financial Offer will be considered to be invalid and will be eliminated from further evaluation.

#### Part 2: SCENARIO (NIS Investments 2023)

Consists of multiple fields (names of actual experts offered etc.) and price boxes in which the rates and the number of person days allotted to each expert consultant must be added, - thereby generating an automated sub-total and finally a total consultant cost for this particular scenario/first project.

**Please note:** It is obligatory to provide a fully costed and detailed financial offer for the Scenario.

$$PP = (((A/P_s) + (C/P_J)) \times 25) + ((T_{SCA}/T_{SC}) \times 50)$$

where

**A** - is the best price of all bidders for person/day rates for Senior Expert

$P_s$  - is the price for a single bidder for person/day rates for Senior Expert

**C** - is the best price of all bidders for person/day rates for Junior Expert

$P_J$  - is the price for a single bidder for person/day rates for Junior Expert

$T_{SCA}$  - is the best Scenario price of all bidders

$T_{SC}$  - is the Scenario price for a single bidder

**Please note:** If any price box is left blank by the tenderer then the Financial Offer will 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:

$$TWP = (QP \times 0.7) + (PP \times 0.3)$$

Where;

**QP** = Qualitative points

**PP** = 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 **4<sup>th</sup> November 2022 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](mailto: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: six months 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: **Supporting analysis of cybersecurity investments and business resilience**

**ENISA F-PDI-22-T37**

#### 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	30 <sup>th</sup> September 2022	
Deadline for request of information to ENISA	28 <sup>th</sup> October 2022	
Last date on which clarifications are issued by ENISA	31 <sup>st</sup> October 2022	
Deadline for <b>electronic reception</b> of offers via <b>e-Submission</b>	<b>3<sup>rd</sup> November 2022</b>	<b>18:00 CET</b> Central European time
Opening of offers	4 <sup>th</sup> November 2022	<b>09:30 CET</b> Central European time
Date for evaluation of offers	TBA	
Notification of award to the selected candidate + 10 day standstill period commences	TBA	
Contract signature	End November 2022	Estimated