OPEN CALL FOR TENDERS

Concluding with: ***Multiple Framework contracts with 're-opening of competition'***

Tender Documentation

"Support services for the Ad-hoc cybersecurity assistance mechanism"

ENISA F-OCU-21-T13

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	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) (hereinafter CSA). ENISA is dedicated to achieving a high common level of cybersecurity across Europe. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, boost resilience of the Union's infrastructure, and ultimately, keep Europe's society and citizens digitally secure.

1.2 SCOPE

The frequency and sophistication of cyberattacks is rising speedily, while at the same time the use of ICT infrastructures and technologies by individuals, organisations, and industries is increasing rapidly. The needs for cybersecurity knowledge and competences exceeds the supply. The EU has to invest in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional. The investments should focus not only on increasing the cybersecurity skillset in the Member States but also on making sure that the different operational communities possess the appropriate capacity to deal with the cyber threat landscape.

The energy that fuels the mill of cybersecurity is information and knowledge. For cybersecurity professionals to be efficient at tackling our objectives, to work in a constantly moving environment – in terms of digital developments as well as with regard to actors – to face the challenges of our time, we need a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.

The Agency shall assist Member States, Union Institutions, bodies, and agencies, as well as various sectors to improve and develop capabilities to respond to cyber threats and incidents, raise resilience and increase preparedness across the Union. Actions to support this activity include support information sharing within the cybersecurity ecosystem and assist in reviewing and developing national level cybersecurity strategies. The legal basis for this activity is Article 6 of the CSA.

The Agency shall, at the request of Member states facilitate handling of incidents or crises, public communication related to such incidents or crisis and testing cooperation plans for such incidents or crisis. The legal basis for this activity is Article 7 of the CSA.

Moreover, the Agency shall provide shall provide strategic long-term analysis, guidance and advice on emerging technologies (such as in the area of artificial intelligence, quantum cryptography, distributed ledgers, cloud computing, edge computing, software development, etc.), cyber threats and threat landscapes, vulnerabilities and risks, and provides topic-specific as well as general assessments on the expected societal, legal, economic and regulatory impact, as well as targeted recommendations to Member States and Union institutions, bodies, offices and agencies. Assessments of the impact as mentioned above, include several aspects and aim at evaluating the potential impact of cybersecurity policies, capacity-building activities, market needs and trends, operational preparedness, etc. They may be both quantitative and qualitative and they need to take into account contextual particularities. These activities leverage on expertise of relevant legal, regulatory, economic and society trends and data by aggregating and analysing information. The legal basis for this activity is Article 9 of the CSA.

1.3 OBJECTIVES

In the context of this framework contract, the Agency's objectives are as follows:

- Empowered and engaged communities across the cybersecurity ecosystem.
- Foresight on emerging and future cybersecurity challenges.
- Efficient and effective cybersecurity information and knowledge management for Europe.
- Cybersecurity as an integral part of EU policies.
- Effective cooperation amongst operational actors within the Union in case of massive cyber incidents.
- Cutting-edge competences and capabilities in cybersecurity across the Union.
- High level of trust in secure digital solutions.
- The Agency shall assist Member States in developing national strategies on the security of network and information systems, where requested pursuant to Article 7(2) of Directive (EU) 2016/1148, and promote the dissemination of those strategies and note the progress in their implementation across the Union in order to promote best practices (Art. 6 (e) of the CSA).
- The Agency shall, at the request of Member states facilitate handling of incidents or crises, public communication related to such incidents or crisis and testing cooperation plans for such incidents or crisis. (Art 7 (4) and (7) of the CSA)
- The Agency shall perform analyses of emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity (Art. 9 (a) of the CSA).

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 to provide support for ENISA's work on developing and implementing an ad-hoc assistance mechanism in case of large-scale cross-border incidents or crises related to cybersecurity. The purpose of the services provided can vary depending on the activity it is meant for. For example, they can be meant for needs and requirements collection and analysis, guidelines and procedures development, provision of experts, setting up database of experts etc.

By means of this Call for Tenders ENISA seeks to contract the services of a minimum of three (3) and maximum of eight (8) competent service providers, which can provide support for such an Ad-hoc assistance mechanism including but not limited to working principles and conditions development, providing relevant expert support and other related activities. The successful bidders should be able to demonstrate significant experience and skills in these fields, with emphasis on the aspects dealt with in the annual ENISA Work Programme[1].

Subject of the tender	Maximum budget
Support services for the Ad-hoc cybersecurity assistance mechanism	A maximum budget of **€800.000,00 (eight hundred and thousand euro)** over the maximum possible period of 4 years
Last date for dispatch of offers	**5th April 2021 until 18:00 CET**

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[2]. 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 UK based entities (and entities outside the EU):

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] https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2021-2023

[2] 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

Securing network and information systems in the European Union has been deemed as a key objective in an effort to keep the EU online economy functional and secure. It is evident that failure to do so could have far-reaching consequences for European citizens and threatens to impact the trust of citizens, the industry and public administration alike.

With the role of ENISA has been further bolstered by means of CSA, the important task of supporting Member states with respect to operational cooperation within the CSIRTs network and contributing to developing a cooperative response at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity, calls for appropriate stakeholders' involvement and support (CSA Art 7(4) and (7)).

Among other activities, ENISA is developing an ad-hoc assistance mechanism to be able to:

- Provide advice in relation to a specific cyber threat.
- Assist in the assessment of incidents.
- Facilitate the technical handling of incidents.
- Provide support in relation to ex-post technical inquiries regarding incidents.
- Support the public communication efforts relating to such incidents or crises.

The purpose of such mechanism is to ensure appropriate support, which is initiated by a request from one or more Member States. The mechanism should be transparent to all parties involved and available as needed. It should observe relevant legal requirements and should be flexible to ensure applicability for all Member States.

In support of the execution of its Work Programme in this field, ENISA is looking to contract external supporting services.

2. PROJECTS PLANNED

ENISA supports the Member States with respect to operational cooperation and cooperative response to large scale-cross border incidents or crises related to cybersecurity and it continues activities with Member States (such as supporting CyClone[3] and CSIRTs network[4] for example).

The tendered services shall cover various aspects that may be required to support ENISA's activities in the area of establishing and supporting an ad-hoc assistance mechanism.

Examples include:

- Analysis of potential needs and requirements of Member States.

[3] https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone

[4] https://csirtsnetwork.eu/

- Analysis of possible incident and crisis management scenarios and relevant case studies in cases of large scale-cross border incidents or crises.
- Risk analysis of establishing and supporting assistance mechanism.
- Supporting the development and implementation of a database of the available expertise on a Union level.
- Development of template of terms of engagement.
- Development of guidelines for assistance.
- Identification and development of relevant processes and procedures.
- Access to external experts.
- Research and documentation of legal and technical aspects of assistance mechanism.
- Identification of possible synergies with other similar mechanisms.
- Support of implementation and improvement of assistance mechanism.
- Creating potential scenarios for exercises/trainings.

3. AREAS OF EXPERTISE

We expect tenderers to have expertise and knowledge in at least several of the following areas:

- Relevant EU legislation.
- Relevant national legislation.
- Experience in developing processes and procedures related to incident response.
- Providing technical, operational and strategic support and assistance in case of cybersecurity incidents to third parties.
- Practical experience in handling large-scale cybersecurity incidents involving multiple stakeholders *(Expertise in the domain of how the CSIRTs Network and/or MS handle cyber incidents will be considered as advantageous).*
- Experience in service areas (including services in each area) covered by CSIRT Services Framework in particular:
    - Information Security Incident Management.
    - Knowledge transfer.
    - Vulnerability management.
    - Situational awareness.
- Typical attack vectors. Capabilities of types of potential attackers.
- Good knowledge of areas that might be impacted by large-scale incidents (e.g. ICS, IoT, Operators of Essential Services, Digital Service Providers etc.).
- Practical experience in carrying out risk assessments.

- Collecting stakeholders' requirements, aggregating and documenting different opinions and viewpoints.
- Crisis communication.
- Generating technical documentation.
- Presenting complex technical issues to various stakeholders (e.g. operational and political decision makers).

4. DESCRIPTION OF TASKS & SERVICES TO BE PROVIDED

The objectives of the services may take but are not limited to, the following forms:

- Collection and documentation of requirements (surveys, evaluations, input consolidation).
- Information exchange with stakeholders.
- Supporting risk assessments.
- Large scale cybersecurity management including (but not limited to):
    - Artefact and forensic evidence analysis.
    - Mitigation and recovery.
    - Incident handling and/or coordination.
    - Crisis management.
- Supporting post fact analysis and implementation of lessons learned.
- Addressing sub-tasks in own responsibility.
- Coordination of working teams.
- Creating document drafts.
- Review and consolidation of work results and documents.
- Creating summaries as document or presentation.

The list of the above-mentioned tasks associated with the provision of consultancy services is made for illustration purposes only and it can be extended or reduced as required by operational needs. Successful tenderers may be required to carry out any additional service in support of the above-mentioned objectives in order to warrant and effectively deliver quality material and outputs, while supporting objectives laid out in the ENISA Work Program on operational cooperation.

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 individual tenders launched under this framework contract.

5. POOL OF EXPERTS AND EXPERT PROFILES

The successful tenderers 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 future project. Experts might need to undergo specific vetting process depending on the future project (e.g. security clearances).

The pool shall comprise experts of both junior and senior profiles. Prospective tenderers are encouraged to provide only the CVs of experts deemed relevant and experienced on the above-mentioned topics.

For this call in particular, we expect that applicants should include **at least five (5)** 'Senior Experts' and **at least five (5)** 'Junior Experts' (see below):

5.1 JUNIOR EXPERT PROFILE

The **Junior Expert** shall have:

- Sound knowledge and expertise in several topics listed under "Areas of expertise" (when listing knowledge and expertise it should be identified at least at the level of service from CSIRT Services Framework, e.g. Service area: Information Security Incident Management Service: Artefact and forensic evidence analysis).
- Minimum 2 years of professional experience in the targeted areas.
- Very good writing skills and ability to draft technical reports.
- Excellent communication and presentation skills.
- Advanced level in both written and spoken English (i.e. at least C1 level of the European Reference Framework).

Advantageous:

- Sound knowledge of the EU, Member States' and international legal frameworks on cybersecurity at large.
- A postgraduate level of education associated with cybersecurity.
- Professional qualifications in the area of cybersecurity.
- Interdisciplinary knowledge of areas related to cybersecurity.
- A background in participation to working groups, experience in preparing presentations in relation to cybersecurity.
- Experience in the field of Cybersecurity incident management.
- Experience in the field of crisis management.

5.2 SENIOR EXPERT PROFILE

The **Senior Expert** shall have:

- Expert knowledge and at least 5 years of professional experience in several topics listed under “Areas of expertise” (when listing knowledge and expertise it should be identified at least at the level of service from CSIRT Services Framework, e.g. Service area: Information Security Incident Management Service: Artefact and forensic evidence analysis).
- Project management skills and experience as team leader.
- Excellent writing skills and ability to draft technical reports.
- Excellent communication and presentation skills.
- Advanced level in both written and spoken English (i.e. at least C1 level of the European Reference Framework).

Advantageous:

- Sound knowledge of the EU, Member States’ and international legal frameworks on cybersecurity at large.
- Professional qualifications in the area of cybersecurity.
- Interdisciplinary knowledge of areas related to cybersecurity.
- A background in participating in or pro-actively leading working groups, experience in preparing presentations in relation to cybersecurity.
- Senior role in the management of large-scale cybersecurity incidents.

6. CONTENT AND PRESENTATION 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 include the following:

- Presentation of tender proposal.
- Evidence demonstrating expertise in the fields covered by this call for tender.
- Examples of relevant previous projects.
- CVs of experts offered.
- Management practices, planning and resource allocation to tasks and experts.
- Project management method that will be used for projects under this framework contract, explaining how possible projects would be carried out efficiently and effectively.
- The procedure for the provision of consultants (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 quality assurance 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.

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

7. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

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

Prices 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 'Request for offers'. These costs will be 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 Proposals' 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://ec.europa.eu/europeaid/work/procedures/implementation/per_diems/index_en.htm

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 cannot exceed **eight hundred thousand Euros (€ 800,000.00)** over a maximum possible period of 4 years.

It is important to note that the amount stated above applies to **all** framework contracts signed under the 'multiple framework contracts' system in total and not for each framework contract. There will be a minimum of three and a maximum of eight 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 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[5] ('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[6] (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.
- 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.

[5] 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

[6] 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)[7], 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

[7] 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. PERIOD OF VALIDITY OF THE TENDER

Tenderers must enclose a confirmation that the prices given are valid for (90) ninety days from the date of submission of the tender.

15. 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.

16. PAYMENT ARRANGEMENTS

Payments under the Contract shall be carried out within 60 days of submission of an invoice accompanying the final report or deliverable based on the conditions set out in the draft contract. One single payment will be made after receipt and approval of the deliverables by ENISA. An invoice must specify the specific deliverables covered. A note that accompanies the final deliverables must present

the resources used for each of the deliverables presented. Time sheets should be submitted as appropriate.

17. CONTRACTUAL DETAILS

A Framework Service Contract will be proposed to the successful candidates. Selection of candidates and / or signature of the Framework Service Contracts 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 twice for a maximum of three 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 'Re-opening of Competition' 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.*

18. PROVISION OF SERVICES - RE-OPENING OF COMPETITION

At the conclusion of this tender procedure, at least 3 and up to 8 contractors will be awarded multiple framework contracts. These contractors will then be eligible to bid for specific future projects based on the 'Re-opening of Competition' procedure, which is explained below:

ENISA launches a 'Request for Proposals' (tender procedure) on a specific subject matter to each of the contractors awarded a framework contract. 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.

- The Framework Contractors will be required to respond typically within 10 - 14 working days with a detailed technical proposal. 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 all offers received by the closing date for reception of proposals. A Specific Contract will be awarded to the best offer in terms of the following award criteria:

  Quality:

    - Compliance with the technical description: *50%*
    - Quality of the proposal to provide the requested services: *50%*

  Price:

  Number of person-days and price per person-day required to complete the project *(can be lower but NOT higher than prices given in original tender)*

  PB = (Person-days x person-day price)

  The Quality/Price ratio will be set at 70/30.

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 IV) 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.

PLEASE NOTE: *ENISA, as a decentralised regulatory agency, cannot accept economic operators from 'Third countries' as members of a grouping (consortium). This restriction does not extend to their use as subcontractors*.

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.

Hand written or electronic signature of the consortium leader who submits the tender is not required, since the signature of the ***e-Submission 'Tender Preparation Report'*** implies that all included documents are signed by this party.

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[8] 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.

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

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[9], 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. The Legal Entity Form needs to be signed by participating parties that are not signing the '***Tender Preparation Report'***.

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.

[9] *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*

(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

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[10].

- 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)*

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

- In the box labelled ***'Total amount'*** – again simply add the amount Total P_B from your Financial Offer form

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 successive stages.

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 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".

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 II 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[11].

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 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 PROFESSIONAL INFORMATION

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 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 **€200.000,00 (two thousand euro)**:

[11] 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

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 **€200.000,00**.

(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

These criteria relate to the Tenderer's or subcontractor's skill, efficiency, experience, reliability and similar circumstances. Tenderers are required to prove that they have sufficient technical and professional capacity to perform the contract by providing the following documentation:

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 cybersecurity incident management with at least **four (4) projects** delivered in this field in the last five years, each with a **minimum value of €30,000.00.**
- The tenderer must prove experience of working and drafting reports in the English language with at least four (4) projects delivered in this field in the last five years, showing the necessary language coverage.
- 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: survey techniques, data collection, 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 **related** services provided in the past five years, with **provable evidence**.
- 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.	**Organizational and methodological quality of the offer**	Suitability and strength of the proposal as measured against the requirements of the illustrative experience on the tasks in terms of completeness and proposed effort. The degree to which the methodology is suited to the needs set out by ENISA, including risk management measures.	25
2.	**Technical quality**	Quality of the offer in terms of technical understanding of the services required.	50
3.	**Quality control measures**	This criterion will assess the quality control system applied to the management of the framework contract concerning the quality of the deliverables, the language quality check, and continuity of the service in case of absence of a member of the team. It should be noted that submitting a generic quality control system will result in a low score.	25
Total Qualitative Points (QP)			**100**

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 **75/100** 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 four (4) price boxes, which shall be completed with a monetary amount by the tenderer.

PS = **(P1 + P2)** will then be used in the price formula as shown below

PJ = **(P3 + P4)** will then be used in the price formula as shown below

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.

PP =[(A/ PS) * 0,5 + (C/ PJ) * 0,5] * 100

where

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

PS - 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

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

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 on **6th April 2021 at 10:30 EET Eastern European Time (Greek local time)** at ENISA Athens office, 1 Vasilissis Sofias Street, Maroussi 151 24 Attiki, Greece.

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: "**Support services for the Ad-hoc cybersecurity assistance mechanism"**

ENISA F-OCU-21-T13

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	29th March 2021	
Deadline for request of information to ENISA	30th March 2021	
Last date on which clarifications are issued by ENISA	5th April 2021	
Deadline for **electronic reception** of offers via ***e-Submission***	**5th April 2021**	**18:00 CET** Central European time
Opening of offers	6th April 2021	**10:30 EET** Eastern European **(Greek local)** Time
Date for evaluation of offers	TBA	TBA
Notification of award to the selected candidate + 10 day standstill period commences	TBA	Estimated
Contract signature	Early May	Estimated