OPEN CALL FOR TENDERS

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

Tender Specifications

for

"Supporting Cybersecurity for Transport sector activities"

ENISA F-COD-19-T13

LOT 1 – Cybersecurity for the MARITIME sector

LOT 2 - Cybersecurity for the RAILWAYS sector

Part 1 **Introduction to ENISA**

Part 2 **Terms of Reference**

Part 3 **Tender Specifications**

Annex I	Legal Entity & Financial ID Forms
Annex II	Declaration on honour on exclusion criteria and selection criteria
Annex III	Financial Offer form
Annex IV	Draft Framework Service contract
Annex V	Power of Attorney for Consortium Form
Annex VI	Sub-Contractors Form
Annex VII	eSubmission_Quick reference guide for the Economic Operators

e-Submission

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

CONTENTS

PART 1 INTRODUCTION TO ENISA

1. Background on ENISA

1.1 Introduction

E-communication infrastructures and online services are essential factors, both directly and indirectly, in economic and societal development. They play a vital role for society and have in themselves become ubiquitous utilities in the same way as electricity or water supplies also constitute vital factors in the delivery of electricity, water and other critical services. Communications networks function as social and innovation catalysts, multiplying the impact of technology and shaping consumer behaviours, business models, industries, as well as citizenship and political participation. Their disruption has the potential to cause considerable physical, social and economic damage, underlining the importance of measures to increase protection and resilience aimed at ensuring continuity of critical services. The security of electronic infrastructures and services, in particular their integrity, availability and confidentiality, faces continuously expanding challenges which relate, inter alia, to the individual components of the communications infrastructure and the software controlling those components, the infrastructure overall and the services provided through that infrastructure. This is of increasing concern to society not least because of the possibility of problems due to system complexity, malfunctions, systemic failures, accidents, mistakes and attacks that may have consequences for the electronic and physical infrastructure, which delivers services critical to the well-being of European citizens.

1.2 Scope

The European Union Agency for Network and Information Security (ENISA, hereinafter 'the Agency') was established in order to undertake the tasks assigned to it for the purpose of contributing to a high level of network and information security within the Union and in order to raise awareness of network and information security and to develop and promote a culture, of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organisations in the Union, thus contributing to the establishment and proper functioning of the internal market.[1]

1.3 Objectives

The Agency's objectives are as follows:

- The Agency shall develop and maintain a high level of expertise.
- The Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security.
- The Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market.
- The Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents.
- The Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors.

2. Additional Information

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

[1] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

PART 2 TERMS OF REFERENCE

I. SCOPE OF THIS TENDER

The purpose of this Call for Tenders is to provide support for the work of ENISA in the area of Transport Security, throughout the years 2019 - 2021.

- **LOT 1 – Maritime:** ENISA envisages around 1-3 projects per year
- **LOT 2 – Railways:** ENISA envisages around 1-3 projects per year,

Examples of topics for projects are - cybersecurity for port facilities, security & resilience for railway undertakings, baseline security requirements for rail sector etc.

By means of this Call for Tenders ENISA seeks to contract the services of a minimum of two (2) and maximum of five (5) service providers (**PER LOT**), which can provide support in the field of Transport Security. The successful bidders 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).

You may choose to bid for **just one LOT, or both LOTS with SEPARATE offers**.

LOT No	Subject of the tender	Maximum budget
LOT 1	**Supporting Cybersecurity for the MARITIME sector**	A maximum budget of **€250.000,00 (two hundred and fifty thousand euro)** over the maximum possible period of 3 years
LOT 2	**Supporting Cybersecurity for the RAILWAYS sector**	A maximum budget of **€250.000,00 (two hundred and fifty thousand euro)** over the maximum possible period of 3 years

PLEASE NOTE: *This tender procedure is limited to tenderers which are legally incorporated in a member state of the European Union/EEA, or which have an incorporated subsidiary in one of the EU/EEA member states. (The Agreement on Government Procurement (GPA) does not apply to EU Regulatory Agencies.)*

IMPORTANT!
Provisions relating to BREXIT
For British candidates or tenderers:

Please be aware that after the UK's withdrawal from the EU, the rules of access to EU procurement procedures of economic operators established in third countries will apply to candidates or tenderers from the UK depending on the outcome of the negotiations.

In case such access is not provided by legal provisions in force candidates or tenderers from the UK could be rejected from the procurement procedure.

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

II. e-Submission application guide

You must submit your tender electronically via the e-Submission application available from the e-Tendering website before the time limit for receipt of tenders.

The e-Submission application allows economic operators to respond to calls for tenders by preparing their tenders electronically in a structured and secured way, and submitting their tenders electronically. The e-Tendering is the starting point for launching the e-Submission application.

Make sure you submit your tender on time: you are advised to start completing your tender early. To avoid any complications with regard to late receipt/non receipt of tenders within the deadline, please ensure that you submit your tender at least several hours before the deadline. A tender received after the deadline indicated in the procurement documents will be rejected.

1. How to Submit your Tender in e-Submission

You can access the e-Submission application via the corresponding call for tender in TED e-Tendering. To have access to e-Submission, you will need to "Subscribe to call for tenders" on TED e-Tendering first. To subscribe, you will need to login with your an EU Login[2]. In case you don't have an EU Login, you can create an account anytime. For more information see the EU login help. After logging in with your EU Login password, the e-Tendering page for the specific tender will then display a button 'submit your tender' from which you will be able to access the e-Submission application.

1(a) Information to be filled in

In the e-Submission application, fill in and upload all necessary fields and documents as appropriate. All tenders must be clear, complete and consistent with all the requirements laid down in Part 2 of this document, including:

- **Signed declaration on Honour(s).** The tenderer, and all members of a joint tender, including subcontractors – if applicable – must upload the signed and dated declaration on honour(s) using the template provided in annex to this document,
- **Exclusion criteria**. If requested in Part 2 Section 3.1 of this document, the tenderer and all members of a joint tender including subcontractors – if applicable – must provide the documentary evidence for exclusion criteria,
- **Selection criteria.** If requested in Part 2 Section 3.2 of this document, the tenderer and all members of a joint tender including subcontractors – if applicable –, must provide the documentary evidence for selection criteria
- **Technical tender.** It must address all the requirements laid down in the Terms of Reference or Technical Specification,
- **Financial tender** The complete financial tender, including the breakdown of the price as provided in the Tender Specifications,

[2] Previously called European Commission authentication system (ECAS)

For detailed instructions on how to submit your tender, see Annex VII - 'Quick Reference Guide for Economic Operators', where you will find:

- Technical requirements for using e-Submission,
- Step-by-step guide to help you submit your tender,
- A link to the test environment for submitting call for tenders,
- Important advice and information,
- How to get technical support

***Please make sure all required documents and evidence are submitted with your tender*.**

1(b) Documents to be signed and dated while creating your Tender

The following documents must be signed and dated during the creation of your tender in e-Submission:

- **Declaration on honour(s).** The tenderer, and all members of a joint tender, including subcontractors must sign and date this declaration. The declaration on honour must be converted to PDF format and then signed by an authorised representative of each member with advanced electronic signature based on qualified certificates, or by hand.
- **Tender Report.** This report is generated by e-Submission while you are completing your tender and it contains the list of documents that you submit. The sole tenderer's or leader's authorised representative(s) must sign the report.

The documents must be signed using any of the following 2 methods:

- *Electronically signed,* in this case you must sign with *an advanced electronic signature based on qualified certificates*.

- *Hand signature*, in this case, you must print the documents and the authorised representative must hand-sign and then scan the documents so they can be uploaded into the system.

  In case of a joint tender, the leader must collect all the original declarations signed by hand by the members of the group and keep them on file together with the Tender Report, if the latter was also signed by hand. The Contracting Authority reserves the right to request these hand-signed originals to be sent via postal service/courier to the address shown in point 5 below. The successful tenderer will in any case be formally requested to provide these originals as well as other documentary evidence required before signature of contract.

2. Re-submission or alternative tender

After submitting a tender, but within the time limit for receipt of tenders, you may still submit a new version of your tender. You must formally notify by that the previous tender is withdrawn. You are also entitled to send several tenders to one call for tenders.

The notification must be sent to address indicated in 'section 5. Contact the Contracting Authority' (below), stating the reference to the call for tenders and the Tender ID you wish to withdraw.
If you submit a new Tender you must include ALL your Tender documents AGAIN, including the Qualification and Tender documents.

3. Withdrawal of tenders

If after submitting a tender, you wish to completely withdraw your tender, you must formally notify that you wish to withdraw your submitted Tender(s).This notification must be signed by the same authorised legal representative(s) who previously signed the tender(s) in question.
The notification must be sent to address indicated in the section 'section 5. Contact the Contracting Authority' (below), stating the reference to the call for tenders and the Tender ID(s) you wish to withdraw.

4. Deadline for receipt of tenders

The tender (including all documents) must be fully uploaded and received before the deadline for receipt of tenders, as indicated in the invitation to tender.

Please note that you are responsible to ensure that your full tender reaches the destination in due time. In case of problems with the submission of the electronic tender, we recommend that you call the 'helpdesk' in reasonable time before the time limit for receipt. The time it takes to submit the tender and upload all your documents may vary considerably depending on the number of concurrent submissions by other economic operators, the size of your tender and the type of internet service you are using.

If the contracting authority detects technical faults in the functioning of the electronic equipment used for submitting and receiving tenders due to which it is impossible to electronically submit and receive tenders, you will be informed of the extension of the time limit by the contracting authority at the e-Tendering link for this particular tender.

5. Contact the Contracting Authority

- When requested, original hand signed documentation must be sent by postal service/courier, to the following address:
  [*Insert tender title and reference*]
  ENISA
  For the attention of the Procurement Officer
  1 Vasilissis Sofias Street,
  Maroussi 15124,
  Greece
- Notifications for re-submission or withdrawal of tenders must be sent to:
  procurement@enisa.europa.eu
  When communicating state the reference to the call for tenders and if applicable, the Tender ID.

6. Get Technical help

In order to get technical help please consult the Quick Reference Guide for Economic Operators or directly contact us by consulting the footer section on e-Submission application.

7. TEST environment for e-Submission application

In order to familiarise yourself with the system and to test whether your workstation configuration is working correctly with our environment, you are invited to access the ***test environment***:

https://webgate.ec.europa.eu/esubmission/index.jsp?CFTUUID=TEST01CFT201706

III. Explanation of 'REOPENING OF COMPETITION' Procedure

Framework contracts (FWC) will be concluded with minimum 2 and maximum 5 successful tenderers as a result of the present Open tender procedure.

During the subsequent implementation period of the FWC, for each individual project, the successful framework contractors will be exclusively invited to submit an offer. When submitting an offer for a specific contract, the framework contractor will respect the maximum unit prices on which basis it won the framework contract. The framework contractor may however decide to offer reduced unit prices for any particular specific contract. The contracting authority will choose the offer with best value for money for the project on the basis of the technical quality of the offer and the price of the services, and will conclude a specific contract with that framework contractor.

This 'Reopening of Competition' procedure will be conducted separately and independently for each project leading to a specific contract, thus ensuring that framework contractors have an equal opportunity on each occasion to be selected as the best offer based on their technical offer.

e-PRIOR Supplier Portal

DG Informatics (DIGIT) is developing under the ISA (Interoperability Solutions for European Public Administrations) programme a number of e-Procurement solutions for the European Commission and its Agencies.

The e-PRIOR Supplier Portal is accessible from anywhere through the Web to authorised Suppliers and currently hosts, among others, the following applications:

- e-Submission
- e-Request
- e-Invoicing

ENISA has implemented the electronic offer submission system called '*e-Request'* specifically for the 'reopening of competition' tender procedures. It is therefore emphasised that the successful contractors for this procedure will be required to use this *e-Request* application to submit their offers.

LOT 1 – Cybersecurity for the MARITIME sector

1.1 BACKGROUND INFORMATION

ENISA's past work on Cybersecurity for Maritime:

Previous ENISA work on Cybersecurity for the Maritime sector:

- Cybersecurity aspects in the maritime sector[3] (2011) was the first ever report dealing with the cybersecurity challenges in the Maritime sector.
- Intelligent Transport systems cybersecurity[4] (2016) highlights the critical assets of Intelligent public transport systems and gives an overview of existing security measures.

ENISA's work on supporting the EU CIIP activities:

ENISA assists Union institutions, agencies and bodies, as well as Member States, in developing and implementing Union policies related to cybersecurity, including sectorial policies on cybersecurity.

In July 2016 the Network and Information Security (NIS) Directive, the first piece of European legislation on cybersecurity, was voted. This directive provides legal measures to boost the overall level of cybersecurity in the European Union by increasing the cybersecurity capabilities in the Member States, enhancing cooperation on cybersecurity among the Member States, and require operators of essential services in the energy sector to take appropriate security measures and report major incidents to the national authorities. Once adopted and implemented, the NIS Directive will benefit citizens, as well as government and businesses, which will be able to rely on more secure digital networks and infrastructure to provide their essential services.

ENISA, as the EU's cyber security agency, will play a significant role in the implementation process of the new regulation, mostly by acting as a central hub for knowledge exchange and by providing support to all types of stakeholders involved in the process. The agency is mentioned several times within the directive having the following responsibilities:

- Assistance for MS and the EU Commission by providing its expertise and advice and by facilitating exchange of best practices.
- Assistance for MS in developing national NIS strategies, a task already started several years ago.
- Participation within the Cooperation Group.
- Support EU Commission in developing security and notification requirements for ESPs and DSPs.
- Assistance for MS in developing national CSIRTs, a process that has been successfully going on for some years now
- Coordination/secretariat/Active Support of the CSIRT network.
- Advices and guidelines regarding standardization in NIS security, together with MS.

[3] https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1
[4] https://www.enisa.europa.eu/publications/good-practices-recommendations

The Cybersecurity Act was agreed in 2018 giving ENISA a new permanent mandate, setting the Cybersecurity agency in the forefront. ENISA is tasked (among others) to promote the consistent implementation of the relevant cybersecurity legal framework, in particular the effective implementation of the NIS Directive and other relevant legal instruments containing cybersecurity aspects, which is essential in order to increase cyber resilience. The starting point are the sectors described in Annex II of the NISD, which splits Transport in Aviation, Rail, Maritime and Road.

In this context, ENISA has established a working group on Cybersecurity for Transport: the TRANSSEC. The goal is to provide the opportunity for relevant stakeholders to address important issues to ENISA in its work enhancing cybersecurity in the Maritime sector, and vice versa the opportunity to ENISA to consult operational actors and identify suggestions and ideas

1.2 PROJECTS PLANNED FOR 2019

Without this being binding on ENISA, it is envisaged that the following topics based on the 2019 Work Programme in the area of Cybersecurity in the Maritime sector, will be tendered mid-2019 to the successful framework contractors:

- Good practices for the maritime sector (ports security)

1.3 AREAS OF EXPERTISE

We expect tenderers to have expertise and knowledge on the following topics.

- Policy and regulatory issues related to the resilience of critical infrastructures and services as well as Maritime cybersecurity at national, European and International (e.g. IMO) level.
- Network and information security of Maritime infrastructures and services.
- Working with maritime sector stakeholders/organisations such as, though not limited to, ports (including port authorities, port facilities, terminals etc.), shipping companies, vessel traffic services, national maritime authorities, classification societies etc.
- Risk management practices/methodologies, regulations, standards, guidelines, good practices specific to the maritime sector (e.g. ISPS)
- ICS-SCADA security issues e.g. OT security, IT/OT convergence etc.
- Essential service (transport sector) operations and security practices and knowledge of the regulatory framework e.g. NIS Directive, the GDPR etc.
- CIIP and/or Maritime security good practice guidelines and standards e.g. ENISA good practice guides, IEC 62443, ISO 27001, ISO 27002, ISO 27019, BIMCO guidelines, NERC CIP standards, ANSI/ISA 99 etc.
- Network and information security issues e.g. internet and web security, cryptography, testing, security management etc.
- Infrastructure security and resilience and CIIP issues like Public Key Infrastructures (PKI) and core protocols e.g. BGP, DNS etc.

1.4 DESCRIPTION OF TASKS & SERVICES TO BE PROVIDED

The objectives of the consultancy services in the area of threat analysis may take but are not limited to, the following forms:

- Perform stocktaking on the topic mentioned above; relevant existing literature, reports, white papers, legislation, policies, strategies, initiatives and other research projects.
- Identify relevant stakeholders and engage them in dialogue on the topics mentioned above, including experts from port authorities/facilities, shipping companies, vessel traffic services, industry associations, standards bodies, certification organisations, National Regulatory Authorities, associations, classification societies, government organizations, large enterprises, etc.
- Design and implement interviews, surveys, questionnaires with relevant stakeholders (conducted face-to-face, via telephone or on-line means, etc.) on the topic mentioned above;
- Analyse and present the results from interviews, surveys and questionnaires.
- Draft reports on the basis of information collected (via interviews and surveys) or on the basis of desk studies;
- Assess the impact of policies and regulations on the Maritime market;
- Perform SWOT analysis for various kinds of technical and organisational cases, including emerging technologies and application;
- Make specific recommendations on practices (good practices, best practices) and operational requirements to address identified issues in relation to port security;
- Validate findings, results, good practices and recommendations with stakeholders;
- Organize or contribute to the organisation of workshops and the drafting of minutes of the workshops;
- Present effectively achieved results by using presentation techniques (paper documents, on-line documents, slides, demonstrators, graphs, videos, etc.);
- Compile collection of relevant contacts;
- Update existing inventories, reports, studies, surveys, etc.

The list of tasks connected to the provision of consultancy services is indicative. The successful tenderers may be required to carry out any additional service in support of the above-mentioned objectives in order to guarantee efficient and effective delivery of quality material and contribute to the achievement of 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 individual tenders launched under this framework contract

1.5 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 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):

1.5.1 Junior Expert profile

The Junior Expert shall have:

- Minimum 2 years of professional experience in the field of network and information security and/or in Maritime infrastructure and systems security;
- Minimum 2 years of prior experience (academic or professional) with technical aspects of Maritime infrastructure and systems or hands-on experience in Maritime infrastructures and systems;
- 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 EU directives, EU national laws, and international laws concerning network and information security (NIS) and more specifically laws and secondary laws relevant for Maritime;
- Experience in pre-research or in academic research (literature reviews and desk research);
- Interdisciplinary knowledge of areas related to NIS (e.g. social issues, awareness raising, legal issues, etc.);

1.5.2 Senior Expert profile

The Senior Expert shall have:

- Minimum 5 years of professional experience in the field of network and information security and/or in Maritime infrastructure and systems security;
- Minimum 2 years of prior experience (academic or professional) with technical aspects of Maritime infrastructure and systems or hands-on experience in Maritime infrastructures and systems;
- Experience with research and development projects (EU funded projects, academic research etc.) or consultancy and advisory services;
- Project management skills and experience as team leader;
- Excellent drafting skills and ability to draft technical reports.
- Excellent communication and presentation skills.
- Proficient in both written and spoken English

Advantageous:

- Knowledge of EU directives, EU national laws, and international laws concerning network and information security (NIS) and more specifically laws and secondary laws relevant for Maritime; knowledge of maritime-specific regulations, risk management methodologies, standards, industry guidelines etc.
- Interdisciplinary knowledge of areas related to NIS (e.g. social issues, awareness raising, legal issues, etc.);
- Experience in collecting feedback from stakeholders, performing interviews;
- Experience in dealing with closed technically oriented communities and individuals (incident response teams and experts).

1.6 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;
- 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.

1.7 CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

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

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 proposal following a 'Request for offers' 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 necessarily be 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.

1.8 TENDER RESULT AND ESTIMATED CONTRACT VALUE

The estimated overall maximum contract value without this being binding for ENISA cannot exceed **two hundred and fifty thousand Euros (€ 250,000.00)** over a maximum possible period of 3 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 two and a maximum of five framework contracts signed, if there are a sufficient number of admissible tenderers that meet the award criteria 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(s) in order to increase the maximum amount stated above by up to 50%. This procedure being fully in accordance with Article 134(e) of the Rules of Application (RAP) implementing the EU Financial Regulation (FR)).

LOT 2 – Cybersecurity for the RAILWAY sector

2.1 BACKGROUND INFORMATION

ENISA's work on supporting the EU CIIP activities

ENISA assists Union institutions, agencies and bodies, as well as Member States, in developing and implementing Union policies related to cybersecurity, including sectorial policies on cybersecurity.

In July 2016 the Network and Information Security (NIS) Directive, the first piece of European legislation on cybersecurity, was voted. This directive provides legal measures to boost the overall level of cybersecurity in the European Union by increasing the cybersecurity capabilities in the Member States, enhancing cooperation on cybersecurity among the Member States, and require operators of essential services in the energy sector to take appropriate security measures and report major incidents to the national authorities. Once adopted and implemented, the NIS Directive will benefit citizens, as well as government and businesses, which will be able to rely on more secure digital networks and infrastructure to provide their essential services.

ENISA, as the EU's cyber security agency, will play a significant role in the implementation process of the new regulation, mostly by acting as a central hub for knowledge exchange and by providing support to all types of stakeholders involved in the process. The agency is mentioned several times within the directive having the following responsibilities:

- Assistance for MS and the EU Commission by providing its expertise and advice and by facilitating exchange of best practices.
- Assistance for MS in developing national NIS strategies, a task already started several years ago.
- Participation within the Cooperation Group.
- Support EU Commission in developing security and notification requirements for ESPs and DSPs.
- Assistance for MS in developing national CSIRTs, a process that has been successfully going on for some years now
- Coordination/secretariat/Active Support of the CSIRT network.
- Advices and guidelines regarding standardization in NIS security, together with MS.

The Cybersecurity Act was agreed in 2018 giving ENISA a new permanent mandate, setting the Cybersecurity agency in the forefront. ENISA is tasked (among others) to promote the consistent implementation of the relevant cybersecurity legal framework, in particular the effective implementation of the NIS Directive and other relevant legal instruments containing cybersecurity aspects, which is essential in order to increase cyber resilience. The starting point are the sectors described in Annex II of the NISD, which splits Transport in Aviation, Rail, Maritime and Road.

In this context, ENISA has established a working group on Cybersecurity for Transport: the TRANSSEC. The goal is to provide the opportunity for relevant stakeholders to address important issues to ENISA in its work enhancing cybersecurity in the Maritime sector, and vice versa the opportunity to ENISA to consult operational actors and identify suggestions and ideas

2.2 PROJECTS PLANNED FOR 2019

Without this being binding on ENISA, it is envisaged that the following topics based on the 2019 Work Programme in the area of Cybersecurity in the Rail sector, will be tendered mid-2019 to the successful framework contractors:

- NIS Directive implementation in the Railway sector

2.3 AREAS OF EXPERTISE

We expect tenderers to have expertise and knowledge on the following topics:

- Ecosystems of Rail sector namely of the operators of essential services (as described in Annex II) of the NIS Directive: railway undertakings and infrastructure managers.
- Rail security issues e.g. OT security, IT/OT convergence, etc.
- Policy and regulatory issues related to the resilience of critical infrastructures and services as well as Railway cybersecurity at national and/or European level.
- Essential service (transport sector) operations and security practices and knowledge of the regulatory framework e.g. NIS Directive, the GDPR, the EU Mobility Packages.
- CIIP good practice guidelines and standards e.g. ENISA good practice guides, Shift2Rail activities, CEN CENELEC SC9X, ETSI TC CYBER, Directives on Safety and Interoperability for Rail etc.
- Network and information security of Railway infrastructures and services.
- Policy and regulatory issues related to the resilience of critical infrastructures and services as well as Railway cybersecurity policies at national and/or European level.
- Network and information security issues e.g. internet and web security, cryptography, testing, security management etc.
- Infrastructure security and resilience and CIIP issues like Public Key Infrastructures (PKI) and core protocols e.g. BGP, DNS etc.
- Internet operations in network and security management for large network providers and Internet Exchange Points.

2.4 DESCRIPTION OF TASKS & SERVICES TO BE PROVIDED

The objectives of the consultancy services in the area of threat analysis may take but are not limited to, the following forms:

- Perform stocktaking on the topic mentioned above; relevant existing literature, reports, white papers, legislation, policies, strategies, initiatives and other research projects in relation to railway security.
- Identify relevant stakeholders and engage them in dialogue on the topics mentioned above, including experts from railway undertakings, infrastructure managers, industry associations,

standards bodies, certification organisations, National Regulatory Authorities, associations, government organizations, large enterprises, etc.

- Design and implement interviews, surveys, questionnaires with relevant stakeholders (conducted face-to-face, via telephone or on-line means, etc.) on the topic mentioned above;
- Analyse and present the results from interviews, surveys and questionnaires.
- Draft reports on the basis of information collected (via interviews and surveys) or on the basis of desk studies;
- Assess the impact of policies and regulations on the Rail components market;
- Perform SWOT analysis for various kinds of technical and organisational cases, including emerging technologies and application;
- Make specific recommendations on practices (good practices, best practices) and operational requirements to address identified issues in relation to rail security;
- Validate findings, results, good practices and recommendations with stakeholders;
- Organize or contribute to the organisation of workshops and the drafting of minutes of the workshops;
- Present effectively achieved results by using presentation techniques (paper documents, on-line documents, slides, demonstrators, graphs, videos, etc.);
- Compile collection of relevant contacts;
- Update existing inventories, reports, studies, surveys, etc.
- Possibly create material for publication and dissemination.

The list of tasks connected to the provision of consultancy services is indicative. The successful tenderers may be required to carry out any additional service in support of the above-mentioned objectives in order to guarantee efficient and effective delivery of quality material and contribute to the achievement of ENISA Work Program 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 individual tenders launched under this framework contract

2.5 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 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):

2.5.1 Junior Expert profile

The Junior Expert shall have:

- Minimum 2 years of professional experience in the field of network and information security and/or in Railway infrastructures and systems;
- Minimum 2 years of prior experience (academic or professional) with technical aspects of Railway infrastructure and systems or hands-on experience in Railway infrastructures and systems;
- 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 EU directives, EU national laws, and international laws concerning network and information security (NIS) and more specifically laws and secondary laws relevant for Railways;
- Experience in pre-research or in academic research (literature reviews and desk research);
- Interdisciplinary knowledge of areas related to NIS (e.g. social issues, awareness raising, legal issues, etc.);

2.5.2 Senior Expert profile

The Senior Expert shall have:

- Minimum 5 years of professional experience in the field of network and information security and/or in Railway infrastructure and systems;
- Minimum 2 years of prior experience (academic or professional) with technical aspects of Railway infrastructure and systems or hands-on experience in Railway infrastructures and systems;
- Experience with research and development projects (EU funded projects, academic research etc.) or consultancy and advisory services;
- Project management skills and experience as team leader;
- Excellent drafting skills and ability to draft technical reports.
- Excellent communication and presentation skills.
- Proficient in both written and spoken English

Advantageous:

- Knowledge of EU directives, EU national laws, and international laws concerning network and information security (NIS) and more specifically laws and secondary laws relevant for Railways;
- Interdisciplinary knowledge of areas related to NIS (e.g. social issues, awareness raising, legal issues, etc.);
- Experience in collecting feedback from stakeholders, performing interviews;
- Experience in dealing with closed technically oriented communities and individuals (incident response teams and experts).

2.6 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;
- 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.

2.7 CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

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

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 proposal following a 'Request for offers' 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 necessarily be 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.

2.8 TENDER RESULT AND ESTIMATED CONTRACT VALUE

The estimated overall maximum contract value without this being binding for ENISA cannot exceed **two hundred and fifty thousand Euros (€ 250,000.00)** over a maximum possible period of 3 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 two and a maximum of five framework contracts signed, if there are a sufficient number of admissible tenderers that meet the award criteria 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(s) in order to increase the maximum amount stated above by up to 50%. This procedure being fully in accordance with Article 134(e) of the Rules of Application (RAP) implementing the EU Financial Regulation (FR)).

The following specifications are common to BOTH LOTS:

3 DATA PROTECTION AND TRANSPARENCY

While personal data mainly includes professional contact data, specific conditions may apply depending on the context and the type of personal data collected.

Regarding personal data, the EU data protection applicable on the Agency and its Contractors includes the following instruments:

- 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.

Particular attention needs to be paid to transparency conditions that are applicable in the Agency, as they emanate from the following instrument:

- Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

4 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 attained 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.

5 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.

6 PRICE REVISION

Price revision does not apply to this tender procedure.

7 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.

8 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.

9 PROTOCOL ON PRIVILEGES & IMMUNITIES OF THE EUROPEAN COMMUNITIES

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 Communities. Tenderers must therefore give prices, which are exclusive of any taxes and duties and must indicate the amount of VAT separately.

10 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.

11 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 IV).

Execution of the Framework Contracts will be performed via Specific Contracts following the 'Re-opening of Competition' procedure.

*It should be noted that the **current Regulation and mandate for ENISA expires on 18 June 2020**. No contractual obligations therefore can legally surpass this date, including yearly renewals of framework contracts. Negotiations for a new mandate are currently at their final stage and upon promulgation of a new Regulation, it is anticipated that all existing contractual obligations will be transferred to the new legal entity, including the ability to renew existing contracts.*

***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 section before committing to submitting an offer.*

12 PROVISION OF SERVICES - Re-opening of Competition

At the conclusion of this tender procedure, at least 2 and up to 5 contractors **PER LOT** 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 Offers' (tender procedure) on a specific subject matter to each of the contractors awarded a framework contract. The offer 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 respond typically within 10 - 14 working days with a detailed technical offer. This offer will contain all aspects regarding:

    - Technical content relevant to the specific subject matter
    - Experts offered (*they should be from the pool of experts already offered but an alternative can be offered 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 offers. 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 technical reports.

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.

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[5] 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 IV) 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.

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

2.2 Structure of the tender

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

1) Company identification - data and documentation
2) Qualification - data and documentation;
3) 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.

(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 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 V (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 II)
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 III a (*for Lot 1*) or Annex III b (*for Lot 2*).**

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

- Prices must be quoted in **euros**, 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 IV). 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[6]. The completed Financial Offer form, 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.

[6] In the case of framework contracts, please add the maximum budget given for this tender

3. ASSESSMENT AND AWARD OF THE CONTRACT

The assessment will be based on each tenderer's bid. All the information will be assessed in the 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 one step will pass on to the next step

3.1 EXCLUSION CRITERIA

All tenderers shall provide a 'declaration on their honour' (see Annex II), 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 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.

3.2 SELECTION CRITERIA

The following applies to LOTS 1 and 2 identically *(unless otherwise stated)***:**

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) A statement of the average turnover of the last two (2) financial years for which accounts have been closed. The **minimum annual <u>average</u> turnover** of the tenderer shall be of **50,000.00 EUR**. 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 50,000.00 EUR.

(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 <u>before</u> the tender expiry date.

3.2.3 Technical and professional capacity criteria and evidence

These criteria relate to the Tenderer's (and if applicable) partner's/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 Network Information Security (NIS) related to **Maritime security (FOR LOT 1)** and/or **Railway infrastructures and services (FOR LOT 2)** with at least three (3) projects/deliverables **(per LOT)** delivered in these fields in the last three years, each with a minimum value of € 20,000.00
- 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; 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 1.5.1 *(for Lot 1)* and 2.5.1 *(for Lot 2)*

Senior Expert profiles

As per minimum requirements listed in Part 2 section 1.5.2 (*for Lot 1*) and 2.5.2 (*for Lot 2*)

c) Evidence:

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

- Details of the structure of the organisation
  - List of services (relevant to the area of CIIP services) provided in the past five years, 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

The following award criteria apply to LOTS 1 and 2 identically:

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.	**Rationale, Organisation and Methodology**	Understanding of Terms of Reference, approach, completeness, clarity, methodology, processes, list of activities	30/100
2.	**Relevant experience**	Operational knowledge of the EU landscape related to transport security activities, relevant expertise, appropriate proposed team members' expertise	40/100
3.	**Quality control measures**	This criterion will assess the quality control system applied to the service foreseen in this Terms of Reference 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.	30/100
Total Qualitative Points (QP)			**100**

Tenderers shall elaborate in the technical offer on all points addressed in the technical specifications, bearing also in mind the above indicated award criteria, in order to score as many points against the quality award criteria as possible. The mere repetition of mandatory requirements set out in the technical specifications, without going into detail or without giving any benefit in the technical offer, will only result in a very low score.

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 70% after the quality award criteria 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.

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

The following sub-weightings shall be applied to the above prices:

Senior Experts price	70 %
Junior Experts price	30 %

$$P_P = (A/P_S \times 0{,}70) + (C/P_J \times 0{,}30)$$

where

A - is the cheapest 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 cheapest 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

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 **2nd April 2019 at 11:00 EEST Eastern European Summer 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 3 working days** prior to the opening session.

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 divided into two (2) Lots.

- ***LOT 1*** *Cybersecurity for the MARITIME sector*
- ***LOT 2*** *Cybersecurity for the RAILWAYS sector*

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 regarded as confidential.

5.4 No obligation to award the contract

Initiation of a tendering procedure imposes no obligation on ENISA to award the contract. Should the invitation to tender cover several items or lots, ENISA reserves the right to award a contract for only some of them. ENISA 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 Cybersecurity for Transport sector activities"**

ENISA F-COD-19-T13

- ***LOT 1*** *Cybersecurity for the MARITIME sector*
- ***LOT 2*** *Cybersecurity for the RAILWAYS sector*

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	22nd February 2019	
Deadline for request of information to ENISA	25th March 2019	
Last date on which clarifications are issued by ENISA	26th March 2019	
Deadline for **electronic reception** of offers via ***e-Submission***	**1st April 2019**	**18:00 CEST** Central European Summer time
Opening of offers	2nd April 2019	**11:00 EEST** Eastern European summer **(Greek local)** Time
Date for evaluation of offers	TBA	TBA
Notification of award to the selected candidate + 10 day standstill period commences	Mid-April 2019	Estimated
Contract signature	Early May 2019	Estimated
Registration of each contractor to the **e-Request platform**	TBA	Estimated