OPEN CALL FOR TENDERS

*Concluding with a **Framework service contract***

Tender Documentation

Cyber Threat Intelligence Infrastructure – design, deployment and subscription services

"LOT 1 - CTI Infrastructure - design and deployment"

ENISA F-COD-20-T28

Part 1 **Introduction to ENISA**

Part 2 **Technical Specifications (LOT 1)**

Part 3 **Tender Specifications (LOT 1)**

Annex I	Legal Entity & Financial ID Forms
Annex II	Declaration on honour on exclusion criteria and selection criteria
Annex III (a)	Financial Offer form LOT 1
Annex IV (a)	Draft Framework Service contract
Annex V	Power of Attorney for Consortium Forms
Annex VI	Sub-Contractors Form
Annex VII	Administrative ID and Declaration form

e-Submission

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

CONTENTS

PART 1 ABOUT ENISA

1.1 INTRODUCTION

The European Union Agency for Cybersecurity (ENISA) was established by the European Parliament and the Council Regulation (EU) No 2019/881 of 17 April 2019 (OJ L 151/15, 07.06.2019). ENISA is actively contributing to European cybersecurity policy, in order to support Member States and European Union stakeholders to support a response to large-scale cyber incidents that take place across borders in cases where two or more EU Member States have been affected. This work also contributes to the proper functioning of the Digital Single Market.

1.2 SCOPE

The Agency shall assist the European Commission and EU Member States (EU MS), and in consequence cooperate with the business community, in order to help them to meet the requirements of network and information security, thereby ensuring the smooth functioning of the Internal Market. As described in ENISA regulation, one of the objectives of the agency is to assist the Union institutions, bodies, offices and agencies in developing policies in network and information security, so, including building expertise related to availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems. For instance, the new ENISA regulation mentions the necessity to analyse current and emerging risks (and their components), stating: "*the Agency, in cooperation with Member States and, as appropriate, with statistical bodies and others, collects relevant information*". In particular, under Art. 3, Tasks, d), iii), the new ENISA regulation states that ENISA should enable effective responses to information security risks and threats.

ENISA supports the development and implementation of the European Union's policy and law on matters relating to network and information security (NIS) and assists Member States and European Union institutions, bodies and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis.

Since 2019, following the bringing into force of the Cybersecurity Act (Regulation 2019/881), ENISA is tasked to prepare the 'European cybersecurity certification schemes' that serve as the basis for certification of products, processes and services that support the delivery of the Digital Single Market. The European Cybersecurity Act introduces processes that support the cybersecurity certification of ICT products, processes and services. In particular, it establishes EU wide rules and European schemes for cybersecurity certification of such ICT products, processes and services.

1.3 OBJECTIVES

The Agency's objectives are as follows:

- The Agency shall enhance the capabilities of the cybersecurity community including EU Member States to prevent, to address, and to respond to cybersecurity issues and threats.
- The Agency shall provide assistance and deliver advice to the Commission and EU MS on issues related to cybersecurity falling within its competencies as set out in the Regulation.
- Building on national and EU efforts, the Agency shall develop a high level of expertise.
- The Agency shall use this expertise to stimulate broad cooperation between actors from the public and private sectors.
- The Agency shall assist the Commission, in the technical preparatory work for updating and developing EU legislation in the field of cybersecurity.

2. ADDITIONAL INFORMATION

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

PART 2 TECHNICAL SPECIFICATIONS (LOT 1)

I. SCOPE OF THIS TENDER

The purpose of this Call for Tenders (LOT 1) is to select a service provider to design, develop and implement a Cyber Threat Intelligence digital platform and threat database. The initial project will include the setting up, testing and deployment, while subsequent years shall cover further support and maintenance of the CTI infrastructure including any related ongoing annual costs and expenses, which might occur after the initial deployment of the solution.

PLEASE NOTE: We encourage candidates to collaborate with other service providers either via an ad-hoc consortium/grouping or with specific subcontractors in order to be able to offer the complete range of services requested.

Subject of the tender	Maximum budget
LOT 1 - CTI Infrastructure - design and deployment	A maximum budget of **€190.000,00 (one hundred and ninety thousand euro) in the first year** for design/testing and deployment//handover of project (*including subsequent maintenance services and any licencing costs until end of 1st year*). *As part of* An **overall budget** of **€350.000,00 (three hundred and fifty thousand euro)** over the maximum possible period of 4 years.
Last date for dispatch of offers	**10th November 2020 until 18:00 CET**

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.)*

Provisions relating to BREXIT

For UK candidates or tenderers: Please be aware that following the entry into force of the EU-UK Withdrawal Agreement on 1 February 2020 and in particular Articles 127(6), 137 and 138, the references to natural or legal persons residing or established in a Member State of the European Union are to be understood as including natural or legal persons residing or established in the United Kingdom. UK residents and entities are therefore eligible to participate under this call.

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

1. GENERAL DESCRIPTION OF THE REQUIRED SERVICES

In the past decade, the domain of Cyber Threat intelligence (CTI) became a critical component of organization's defence capability. According to the SANS CTI Survey 2020, the usage and interest in CTI related activities increased. While the use of CTI continuously grew, the approach to build and facilitate such capabilities varied based on organizations and their specific requirements. Historically organizations were mostly consuming and facilitating intelligence or threat feeds from vendors. As more intelligence is getting produced based on organizations' portfolios, the toolset landscape proved to be different for consuming and producing the related data and subsequently the intelligence.

ENISA is aiming for designing and developing a Cyber Threat Intelligence (CTI) digital platform and threat database (infrastructure). The final product of such implementation is an IT-environment that will support the collection, collation, analysis and dissemination of CTI collected from a manageable list of publicly available sources.

The EU Cybersecurity Act mandates ENISA to assist Member States in their efforts to improve the prevention, detection and analysis of cyber threats and incidents (Article 6) and to support operational cooperation at Union level by advising on how to improve their capabilities to prevent, detect and respond to incidents (Article 7).

Having that mission in mind, as well as the importance of CTI in fostering collaboration and cooperation amongst operational communities but also internal cybersecurity-focused teams, ENISA is aiming for designing and developing a platform, that would relevantly contribute to fulfil its mission. Such platform, in its final state after properly delivered and accepted, in broader terms should collect information from several information feeds, open and publicly available, and by eliminating duplicated data, provide a single-pane of glass platform, where information can be transformed into knowledge, either on aggregated or in-depth perspectives. Such platform shall enable daily CTI analysis and creation, advanced visualization, customized dashboards creation, but overall, support and relevantly enhance ENISA's business use cases presented in the next section.

Detailed technical, functional, non-functional and optional requirements are provided in sections below for tenderer reference.

BUSINESS USE CASES

The platform should support but should not be limited to, the following use cases:

Use Case #1 – Empowering ENISA internal teams: based on exclusively publicly available data and feeds, the platform should provide a "one-stop-shop" interface for internal ENISA's teams to search, filter, visualize, add or remove new sources and dashboards, allowing for knowledge creation out of all the data provided by the feeds, supporting each business unit's need for technical layer CTI analytics.

Use Case #2 – Empowering a network of appointed teams across EU involved in incident response: based on exclusively publicly available data and feeds, the platform should provide an overview dashboard with a map and display on top of each country aggregated CTI data. This information should be available to external teams and should not allow any drill-down activity on the displayed information.

In broader terms, an internal pre-analysis stage resulted enabled the identification of several synergies, coming to the conclusion that such platform would be of great value and interest to all cyber-security related business units, either on an operational, tactical of strategic level.

CONTEXT

As a result of internal assessment with various ENISA functions, several requirements have been identified, as well as functionalities and specifications for the CTI platform. The identified/proposed solution should therefore adhere as closely as possible to the requirements identified in the following sub-sections. The tenderer should consider both open sourced and proprietary solutions.

Regarding the list of feeds that should be delivered integrated with the solution by design, ENISA has done previous work on defining open source feeds that would be eligible to be adopted. Such a list[1] can be found on ENISA's "Proactive Detection of Network Security Incidents" GitHub page and it should be considered as reference, but not as a rigid and closed list. It is expected from the contractor to propose, after careful revision and quality analysis, a set of feeds following the methodology presented in the evaluation criteria section (*see section 1.3 Evaluation of external information sources*).

The tenderer should deploy the solution within ENISA's premises, consolidate the chosen platform, integrate feeds and then develop additional features, which might not be present and are required.

Such requirements and corresponding description are presented aiming to aid the tenderer by clarifying the characteristics of the required solution and functionalities.

It should be noted that the identified/proposed solution could be a tool or set of tools deployed as the CTI infrastructure.

The functionalities that are envisaged for the ENISA CTI-Infrastructure are (list is non-exhaustive):

1.1 REQUIREMENTS FOR THE CTI INFRASTRUCTURE

The CTI infrastructure should be:

1.1.1. capable of managing requirements in terms of lists or documents.

1.1.2. capable of providing statistics and KPIs for the different intelligence phases.

1.1.3. able to manage and process Request for Information (RFI) received from stakeholders.

1.1.4. capable of collecting all three types of tactical, operational and strategic intelligence with the main focus on operational and strategic.

1.1.5. capable of collecting and processing a variety of structured or unstructured threat data (i.e. XML, JSON, YAML, CSV, TSV, PDF, DOCX, TXT, Email etc.).

1.1.6. able to collect and manage threat data in standard/known data models and provide compatibility and correlation functions among them (i.e. STIX 1.x, STIX 2.x, OpenIOC, CybOX, IODEF etc.).

[1] https://github.com/enisaeu/IRtools

1.1.7. capable of supporting different transport mechanisms (i.e. HTTP, HTTPS, RSS, Email, SFTP, TAXII, REST API, SMB etc.).

1.1.8. capable of ingesting data from different variety of sources: open source reports, Information Sharing and Analysis Centres (ISACS), commercial intelligence providers, intelligence exchange platforms etc.

1.1.9. capable of integrating with internal and local sources for the purpose of collecting threat data (i.e. OpenCSAM, SIEM, Sandbox, CVE etc.).

1.1.10. capable of indexing collected data.

1.1.11. able to store data at scale.

1.1.12. capable of enabling the administrators to create, schedule and maintain manual and automatic backup procedures for data recovery purposes.

1.1.13. capable of providing data storage management and applying retention policies on the stored data.

1.1.14. able to support different database technologies for storage of the data.

1.1.15. capable of storing data in a secure manner.

1.1.16. capable of processing the collected tactical, operational and strategic intelligence with the focus on operational and strategic.

1.1.17. able to normalise all stored/collected data in a common format/standard/data-model.

1.1.18. able to alert or notify the end-users/analysts for the defined keywords or collected threat data that matches the requirements.

1.1.19. able to support flexible data model (or ontologies) with complex objects to be created, linked, and modified appropriately (i.e. campaigns, threat actors, relationships, etc.).

1.1.20. able to link new data to the existing data via association bindings. This can be in form of identifying relationships between objects as mentioned above.

1.1.21. also capable of extracting keywords or defined objects and entities from unstructured data (i.e. pdf) based on common techniques (i.e. usage of Natural Language Processing).

1.1.22. able to identify duplicated threat data/information and subsequently action on them (automatically) based on the requirements.

1.1.23. able to integrate with known open source and commercial toolset for processing of the collected data (i.e. OpenCTI, MISP, etc.)

1.1.24. equipped with API functionality for enrichment and automation purposes.

1.1.25. capable of exporting aggregated and selected data in a format which is fit for SharePoint portals.

1.1.26. capable of enabling version control for the stored and processed data.

1.1.27. able to maintain and apply taxonomies to threat data manually and automatically as required.

1.1.28. able to maintain and apply data-marking/tagging manually and automatically as required.

1.1.29. capable of applying or enforcing privacy laws, regulations and other required restrictions on the collected and processed data.

1.1.30. capable of providing a human interface for the analysts, preferably over HTTPS and SSH (for administrative purposes).

1.1.31. able to provide searching capability so that the analysts can filter and find relevant information based on the content available.

1.1.32. equipped with knowledge management capability for maintaining, tracking and managing various CTI objects, such as threats, campaigns, actors, incidents etc.

1.1.33. capable of supporting frameworks and models used in threat analysis and risk assessment (i.e. Kill Chain, Diamond Model, MITRE ATT&CK, STRIDE etc.).

1.1.34. able to enable end-users to create custom workflows to implement customized CTI process steps. It could also achieve this by providing integration capabilities with open source and commercial workflow-engines.

1.1.35. capable of integrating with ticketing, collaboration and knowledge management platforms. Alternatively, it could have such bespoke capabilities in its infrastructure independently.

1.1.36. able to allow users to integrate technical information (e.g., IoCs) and non-technical information (e.g., localization, other attributes) in order to create a case-like context for the data under analysis.

1.1.37. capable of defining or providing trend analysis and statistics for enhancing analysis achieved by analysts.

1.1.38. able to enable analysts to monitor and manage strategic bulletins.

1.1.39. capable of providing the end users with the ability to create custom graphical interfaces such as graphs and dashboards.

1.1.40. capable of integrating with 3rd party industry standard tools for data visualisation and link analysis. Alternatively, the infrastructure could have this as a native functionality.

1.1.41. able to export the related/created data or intelligence in structured and unstructured formats (i.e. STIX, XML, JSON, YAML, CSV, TSV, PDF, DOCX, TXT, Email etc.).

1.1.42. capable of providing Role Base Access Control (RBAC) and support implementation of different UIs and information access per role.

1.1.43. integratable with active directory in order to support role based access control.

1.1.44. auditable, especially for admin activities. Logs should be downloaded from the platform itself or transferred automatically to an external repository.

1.1.45. able to provide the mechanisms for sharing of information to internal as well as external stakeholders based on defined criteria.

1.1.46. able to disseminate the information in a predefined way considering timing, frequency, occurrence of predefined conditions, and other requirements.

1.1.47. able to support the export of data in standard formats (e.g. CSV, TXT, PDF, HTML, DOCX, XLSX etc.)

1.1.48. capable of creating trust models for creating different teams and communities within the proposed solution.

1.1.49. capable of sending information to multiple systems (multilateral sharing capability)

1.1.50. capable of supporting standard transfer protocols for information exchange.

1.1.51. able to use tagging for sharing information with specific audience (i.e. peers, communities, circles of trust etc.).

1.1.52. able to support sharing information on the fly, via integration with email client or similar solutions, creating a compressed file with all indicators/TTPs/Observables/objects in order to rapidly share information with multiple entities.

1.1.53. equipped with the right mechanisms for signing and encrypting the information sent to stakeholders.

1.1.54. capable of creating custom workflows to enable multi-step approval for disseminating data in required scenarios. Alternatively, it can integrate with third-party workflow engines for such functionality.

1.1.55. offering the capability of multi-team access and remote administration.

1.1.56. following RSIT's Taxonomy, which is available online2.

1.1.57. It will be advantageous for the CTI infrastructure to be able to apply machine learning, analytics and clustering of the collected/stored data.

1.1.58. The CTI infrastructure could ideally provide auditing capability for the stored, processed and shared threat data and intelligence within the proposed solution.

1.1.59. The CTI infrastructure should support clustering and configuration synchronisation between different instances. Business Continuity Management should be considered.

1.1.60. In order to enhance cyber resilience, an offline backup system should be put in place with different hardware and/or OS (e.g., one virtualized node and a second physical node or two physical nodes with e.g. Solaris and Red Hat)

[2] https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force (accessed September 2020)

1.2. REQUIREMENTS FOR CTI INFRASTRUCTURE PROVIDER (THE CONTRACTOR)

The CTI Infrastructure Provider (the contractor) should:

1.2.1. propose a suitable architecture for integration to the ENISA infrastructure.

1.2.2. consider that the solution requires a multi-purpose environment. For instance, one environment can be deployed for training and testing purposes and another environment for production.

1.2.3. be capable of transferring related licenses and ownerships to ENISA or ENISA's approved contractors for strategic maintenance and ownership purposes.

1.2.4. provide relevant processes and procedures for handling credentials during the PoC and final deployment of the solution. It should also provide a process of "hand-over" for credentials and related access levels.

1.2.5. provide the details of any related ongoing annual costs and expenses which might occur after the initial deployment of the solution.

1.2.6. provide their capabilities and services for further support and maintenance of the CTI infrastructure (including related expenses).

1.3. EVALUATION OF EXTERNAL INFORMATION SOURCES

For the evaluation of the data feeds to be used in the solution, the contractor is required to provide a list of the proposed data feeds and to evaluate them using the following criteria, which are the same ones used in the study "Proactive detection of Incidents[3]."

a) Timeliness

Whether the source provides information that is recent enough to be useful for proactive detection.

- **Poor:** Information provided by the sources is not recent enough to be effective for proactive detection.
- **Excellent:** The sources provide current information about threats with low delay.

b) Accuracy

Trustworthiness of the source, especially with regard to false positives. False positives in this context means that the team would see false alarms if the information from the source is used for monitoring.

- **Poor:** The number of potential false positives means that all results need to be verified manually.
- **Excellent:** In most cases, analysts can be certain that the information is correct.

[3] https://www.enisa.europa.eu/publications/proactive-detection-measures-and-information-sources

c) Ease of use

Whether the team needs much expertise, effort or other resources to integrate the source with its internal workflows and tooling.

- **Poor:** Analysts need to spend much time to learn how to interpret and use information provided by these sources.
- **Excellent:** Using information provided by the sources for proactive detection is easy and does not require specialized knowledge.

d) Data volume

Expected amount of data provided, relative to other categories.

e) Completeness

Does the level of technical detail is sufficient for early detection purposes?

- **Poor:** The sources do not provide a sufficient level of detail for effective proactive detection.
- **Excellent:** Information provided by the sources contains all relevant details.

For each criteria category, several examples of sources are provided on the GitHub repository[4].

2. TASKS TO BE PERFORMED

TASKS: SOLUTION ARCHITECTURE, DESIGN AND PHASES

The solution architecture and design should be presented by the tenderer to ENISA. Below we provide an overview of tasks, phases and deliverables:

2.1 TASK 1: REQUIREMENT ANALYSIS AND FUNCTIONAL SPECIFICATIONS

- Requirement Analysis: the contractor will engage ENISA teams to understand the requirements and functionalities that are specified for the project. Should perform a first phase of business understanding per each of ENISA's teams, in order to properly contextualize the project and details presented in the current document; All type of requirements will be assessed.

- Functional Specifications: based on the Requirement Analysis, the contractor's team should start identifying functional requirements and specifications for the platform. They should also propose, after careful revision and quality analysis, a set of feeds following the methodology presented in Section 1.3 'Evaluation of external information sources'. The final list for integration should be agreed by ENISA together with the rest of the specifications. Business use cases and models should also be assessed in this phase in order to start preparing a solution test plan.

The task will result in **D1**: 'Identify existing CTI requirements within ENISA'

[4] https://github.com/enisaeu/IRtools

2.2 TASK 2: HIGH LEVEL DESIGN AND BLOCK DIAGRAM OF THE SOLUTION

In this phase, the contractor should be able to start defining the high-level design of the solution and draft the way that the requirements will be met. A high-level block diagram of the solution should be prepared as a result of the assessments performed by the contractor.

The task will result in **D2**: 'High-level solution proposal'

2.3 TASK 3: DETAILED DESIGN AND SOLUTION SPECIFICATION

This is the phase in which the contractor presents its detailed solution based on all requirements and specifies how the solution will implement them. At the end of this phase the contractor is ready to start building the solution and implementing all functionalities. It is, therefore, one of the most important stages of the project and significant interaction and cooperation should exist between both teams.

The task will result in **D3**: 'Solution proposal'

2.4 TASK 4: SOLUTION IMPLEMENTATION

In this phase, the contractor starts implementing the solution based on the information discussed in the previous stage. At this stage the contractor will develop a proof of concept and a minimum viable product – MVP – and submit it for analysis by ENISA.

All development, bug correction and solution building occurs in this stage. It is, therefore the most important stage and it will be finished only when the final phase is completed and the project accepted. It is of utmost importance in this phase to have a clear view on all requirements, risks and have no doubts about the type of solution and business cases required by ENISA. The contractor will consider as the MVP the solution that will implement the first business case. From that point on all phases from testing to the end should be performed for the two business cases.

The task will result in **D4**: 'Solution Implementation'

2.5 TASK 5: TESTING

This task is composed of 5 types of testing and evaluation:

- **Testing Phase:** in this stage of the project, it is up ENISA to develop a set of tests in order to evaluate the compliance level of the solution versus the requirements identified. Advancing to the next phase depends on the type of project methodology used (waterfall or agile – which is up to the contractor to define with ENISA).
- **Solution Integration Testing:** after all testing has been performed it is up to the contractor to perform integrated tests for the overall solution, with ENISA's team. At this phase the solution should already have passed the MVP and been enhanced towards finalization and pre-production evaluation.
- **Overall Solution Testing and Pre-Production Evaluation:** At this stage, the solution is already integrated, and it complies with the several requirements at a given extent. All non-compliant items should be registered and risk analysis should be performed. ENISA's and contractor's teams will both conduct a final test phase to the solution as a whole and evaluate its quality and readiness level towards production.

- **User/ENISA Teams acceptance testing:** in this stage ENISA will invite other stakeholders to functionally test the solution and gather feedback from other teams. ENISA project team will then evaluate with the contractor any additional changes to the solution as a result of given feedback. After overcoming that final testing and re-testing phase, ENISA's team will issue an acceptance form so that the solution can enter the final testing phase before production.
- **Solution Production testing:** in this phase, the solution will be put into production by the contractor and final tests will be performed to evaluate its stability and overall quality. This will be the final phase for feature and requirement testing.

The task will result in **D5**: 'Final testing report'

2.6 TASK 6: OVERALL SOLUTION ACCEPTANCE

Finally, the last phase is the overall acceptance of the solution, which is already in production mode. From this point on, it is up to the contractor to provide support to ENISA users over the platform.

The task will result in **D6**: 'Overall Solution Acceptance'

NB: The selected contractor is advised that some stages might be repeated iteratively until convergence and maximum compliance with the different set of requirements is attained. All phases, especially testing phases will be performed by ENISA with the support from the selected contractor. It is up to the contractor to develop test plans with ENISA prior to any testing phase.

At least, the following test plans are suggested prior to the corresponding phase:

1. User acceptance Test Plan (requirement analysis and overall solution acceptance);
2. Solution/System Test Plan (functional specifications and solution production testing):
3. Integrated Test Plan (solution production testing and solution integration testing);
4. Unit Test Plan (detailed design, solution specification, detailed design and solution specification);
5. Pre-production Assessment (overall solution testing, pre-production evaluation and user/enisa teams acceptance testing).

2.7 TASK 7: POST-SOLUTION DEPLOYMENT REPORT

Following the deployment the contractor should submit a post-solution deployment report containing the following items:

1. Overall Project Report
2. Risk Analysis focusing on feed providers, solution and feed quality
3. Follow-up items to be future developed.

The tenderer should consider this information as a reference.

The task will result in **D7**: 'Post-solution deployment report'

Additional remarks

ENISA expects a detailed description of the project phases, deliverables and testing checkpoints. Additionally, a high and low-level design of the solution architecture should be presented as well as detailed information about the proposed feeds and corresponding information and update frequency.

The developed system should support high-availability and be ready to be deployed in the medium term on two different datacentres to ensure business continuity of the service.

2.8 TASK 8: MAINTENANCE AND SUPPORT

After the finalisation of the installation and deployment of the CTI Infrastructure – planned for end July 2021, the contractor will offer maintenance support and licence costs (if any) for the installed infrastructure **for the rest of the first year** *(i.e. until end of January 2022 if project commenced on 1st Feb 2021).*

For the subsequent years, the contractor will be asked to provide maintenance support and take care of the licence management of the installed tools, on behalf of ENISA. For this reason, a draft Service Level Agreement (SLA) must also be provided as part of your offer.

2.9 TASK 9: PROJECT MANAGEMENT

The main objective of this task is to define and implement appropriate management mechanisms, sound planning and resource allocation according to proven expertise and prior knowledge of the subject.

As part of this task, the prospective contractor should also provide justification for subcontracting, interact with ENISA staff and external experts, and provide regular management reporting. This will ensure the punctual delivery of good quality results.

The prospective contractor is expected to submit to the Agency, prior to the kick off meeting, detailed Gantt Charts and accompanying documentation with sufficient details. These will be negotiated with ENISA and be confirmed as final.

The Gantt charts and related documentation should include:

- Scheduling of all tasks and activities within the tasks.
- Identification of milestones and critical activities.
- Assignment of experts and person days to tasks and activities.
- Identification of possible risks and suggestions to mitigate them.
- Detailed information on the expertise of the contractors on the tasks and topics of this tender, including references to previous relevant projects.
- Detailed CVs of experts proposed to be involved in all the tasks of the project.
- Detailed justification for subcontracting tasks or parts of them. In that case, ENISA requires additional information on the:
    - tasks undertaken by the sub-contractor;

- expertise of the contractor and its experts;
- resources allocated to him/her;
- co-ordination mechanisms among the prime and the sub-contractors;
- risk management method in case of delayed and/or low-quality delivery of sub-contractor's outcomes;
- and official statement of overall responsibility for the whole project and its results by the prime contractor.
- Proposal for a peer-review.

Based on the Gantt chart, the contractor is expected to deliver the following documents regularly:

- Brief bi-weekly progress report on current activities (as defined in the Gantt chart) information on the progress achieved, next steps, possible risks affecting project, and risk mitigation measures;
- Early warning reports, at any time, if emerging risks threaten key milestones of the project and when the Agency needs to either be informed or take a decision;
- Minutes from the bi-weekly teleconferences with ENISA staff on the progress of the project and its tasks;

At least the following communication with the Contractor is expected:

- Regular video or teleconferences via Skype, Lync (every second week, or at more frequent intervals to be agreed upon) on the progress achieved.
- Approximately three meetings with the ENISA expert group should also be planned. Given the current COVID-19 travelling restrictions, these meetings will be performed by means of Video-Conferencing.

3. EXPECTED SKILLS

Considering the specifications of the project, as well as the requirements ENISA expects the tenderer to allocate specialized human resources, with proven experience, at least on the following skills:

- Project management and team coordination experience and objective-oriented profile;
- Very good writing skills and ability to write technical and executive reports;
- Excellent communications and presentation skills.
- Cyber Threat intelligence analysis and creation;
- Software and scripting development;
- Cyber Intelligence and Strategic Information Systems;
- Incident Response;
- Knowledge of CSIRT operations at a national level and specific information needs.
- Implementation of cybersecurity information sharing platforms;
- Experience in cyber report development: threat landscapes, benchmarks, operational and executive.

- Extensive knowledge of open source intelligence (OSINT), open source tools and open source software development.
- Fluent and proficient in both written and spoken English (project interactions with ENISA based on spoken English)
- Extensive knowledge in the area of Cybersecurity.

The following competences would be of added value and scored higher:

- Data Scientist, with experience in the development of dashboards and data visualization;
- Previous experience in data and text mining, as well as Big Data storage and processing;
- Skilled in the development of artificial intelligence and machine learning applications;
- Proficient on design thinking, functional design and information design;
- Previous experience in implementation of OpenCTI platforms or tenderer's proposed platform.
- Familiarity and previous experience with activities performed by ENISA..

4. DURATION

The required effort should start in February 2021 and be finalised and completed by end July 2021.

It is expected that the tasks mentioned above and the deliverables will be performed with some overlap. An indicative execution plan of the above tasks, possibly also including milestones, is as follows:

Activity	Indicative time window of execution	Milestone
Task 1	Start of February 2021	Requirement analysis and functional specifications D1: Identify existing CTI requirements within ENISA
Task 2	End of February 2021	High Level Design and Block Diagram of the Solution D2: High level solution proposal
Task 3	End of March 2021	Detailed Design and Solution specification D3: Solution proposal
Task 4	April - June 2021	Solution Implementation D4: Solution Implementation
Task 5	March - June 2021	Testing D5: Final testing report
Task 6	End of June 2021	Overall solution acceptance D6: Overall Solution Acceptance
Task 7	June - end of July 2021	Post-solution deployment report D7: post-solution deployment report
Task 8	Remainder of 1st year	Delivery of maintenance and (any) licence costs for the remaining months of the 1st year
Task 9	February – July 2021	Project management

ENISA expects the contractor to deliver a project plan detailing the execution of these activities and related deliveries. All the documents (interim and final reports, project management reports etc.) produced in the project shall be in English.

4.1 LIST OF DELIVERABLES

The Contractor is expected to deliver the following services to ENISA:

- **D1:** Identify existing CTI requirements within ENISA
- **D2:** High level solution proposal
- **D3:** Solution proposal
- **D4:** Solution Implementation
- **D5:** Final testing report
- **D6:** Overall Solution Acceptance
- **D7:** Post-solution deployment report
- **D8:** Maintenance and support (12 months)

We expect, given the planning, that the Contractor will need to work in parallel for the aforementioned deliverables.

English is the language to be used for all the reports, articles, documents and material produced.

5. PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS

The execution of the activities will take place at the Contractor's premises. Network based collaborative tools (i.e. videoconferencing) will be used as working methods when needed. It should be considered that the developed and deployed tools or functionalities of the CTI infrastructure will be made available to ENISA during the corresponding phases in the cloud environment.

In order to save project resources, the information exchange will be performed via electronic means, such as e-mail, web and phone conferencing. ENISA will facilitate this information exchange by mediating between the contractor when necessary and especially during the initial phases of the project.

It should be mentioned that the contractor's costs of potential business trips - if needed - should be included in the total offer. ENISA will not additionally reimburse the contractor for taking part in these meetings

6. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER (LOT 1)

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

The technical offer must address each of the following elements as A MINIMUM in order to be considered a valid and conforming offer:

- The tenderer must provide:

  - Detailed specifications on the services required from ENISA;
  - The required information/documentation that ENISA may need to provide for the vendors in order to receive their services
  - Evidence demonstrating expertise in the fields covered by this call for tender;
  - Management practices, planning and resource allocation to tasks and experts;
- The tenderer must include all related project management information including:
  - Gantt chart(s) representing tasks, milestones, project product delivery dates,
  - List of possible risks and mitigation measures,
  - The project quality assurance process,
  - The composition of the Contractor's project team with their exact role in the project,
  - List of similar or relevant projects
  - Project management method that will be used for the project under this framework contract, explaining how it would be carried out efficiently and effectively;
- 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 (LOT 1)

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.

The Financial Offer form requires that you provide a SEPARATE lump sum price for the initial design/deployment and final handover of the CTI Infrastructure project, which shall cover the CTI infrastructure and all related licenses and services for the first 12 months. It is anticipated that the efforts required for this project (for the 12 month period) should reasonably be priced at an amount **not exceeding €190.000,00**

Ongoing yearly services (in years 2 to 4) for the CTI infrastructure including yearly maintenance support and licence management (if applicable) of the installed tools shall be costed by the tenderer using the separate price boxes provided for each type of service. Any other related services (optional) may also be offered and included in the extra boxes provided in the Financial Offer form (*but will not be used in the price formula award criteria)*.

8. TENDER RESULT AND ESTIMATED CONTRACT VALUES (LOT 1)

The result of the evaluation of tenders will be the awarding of a framework service contract. The estimated overall maximum contract value without this being binding for ENISA is **three hundred and fifty thousand Euro (€ 350,000.00)** over a maximum possible period of 4 years.

IMPORTANT: The initial deliverable, which includes the design/deployment and handover of the CTI Infrastructure project, has a maximum allowable contract value of **one hundred and ninety thousand Euro (€190,000.00)** which shall cover the CTI infrastructure and related licenses and maintenance services (for the first 12 months) as mentioned in Section 2. **Please ensure that your offer for the project does NOT exceed this amount.**

The remainder of the contract budget will be used in years 2 to 4 for yearly maintenance support, licence management of the installed tools, and any other services/support that may be required.

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 IV.

- **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

[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

II.9.1 of the draft contract in Annex IVa. 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;
- 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.;

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

- 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 IV is applicable.

Confidentiality:

ENISA will disregard general statements that the whole tender or substantial parts of it contain confidential information. Tenderers need to mark clearly the information they consider confidential and explain why it may not be disclosed. The EU body reserves the right to make its own assessment of the confidential nature of any information contained in the tender.

10. 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 for the duration 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 30 days of submission of an invoice accompanying the final report or deliverable based on the conditions set out in the draft contract.

The 'e-Invoicing Web Portal' of the European Commission shall be used for submitting invoices. Use of this web portal requires the creation of an EU Login (ECAS) account to gain access

The possibility of requests for advance payments and frequency of payments per year shall be discussed and agreed with the winning contractor. 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.

17. CONTRACTUAL DETAILS

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

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

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

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

Execution of the Framework Contract will be performed via Specific Contracts or Order forms. Upon signature of the framework contract by both parties, a specific contract will be immediately signed for the design and deployment project for a period of 12 months.

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

PART 3 TENDER SPECIFICATIONS (LOT 1)

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[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 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.

[8] 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[9], all tenders must provide information and supporting documentation in three 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.

(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:

[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*

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 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.**

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 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[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)*
- 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.

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

3. ASSESSMENT AND AWARD OF THE CONTRACT

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

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/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) 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 **€100.000,00 (one hundred thousand euro)**:

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

(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.

[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

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 related with the areas of expertise listed in Part 2 section 3 with at least two (2) projects delivered in this field within the last three years, each with a **minimum value of € 50,000.00**.
- The tenderer must prove its experience of working in EU countries with at least 2 projects delivered in the last three years.

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) 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 services.

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 for LOT 1		Weighting (max. points)
1.	**Technical compliance**	Compliance with the technical requirements (Part 2 of this document)	40
2.	**Quality and accuracy of content and structure**	Quality of the proposal and accuracy of the description to provide the requested services. Quality of solution offered.	30
3.	**Project Team**	Experience, expertise and relevance of the team proposed for delivering the required platform as well as the ongoing maintenance services	30
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 60/100** overall, after the quality award criteria evaluation phase 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 III (a)** contains three (3) mandatory price boxes (L1a, L1b and L1c), which shall be completed with a monetary amount by the tenderer. Even if you offer zero cost this must be indicated. The general consultancy services price box is not mandatory but would be beneficial to your overall offer.

Please note: If any of the three (3) mandatory price boxes are left blank by the tenderer then the Financial Offer will be considered to be invalid and will be eliminated from further evaluation.

The price points shall be calculated based on the following price scenario formula:

$$P_B = L1a + (3 \times L1b) + (3 \times L1c)$$

$$PP = (PC / PB) \times 100$$

where;

PP = Weighted price points

PC = Cheapest bid price received

PB = Bid price being evaluated

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 11th **November 2020 at 11:30 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 overall Tender ***"Cyber Threat Intelligence Infrastructure – design, deployment and subscription services"*** is divided into 3 Lots.

Lot 1: CTI Infrastructure - design and deployment' ***(this document)***

Lot 2: Design of CTI objects

Lot 3: Delivery of subscription services related to the Operational Cooperation of ENISA

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.