ANNEX A

SCENARIO - Terms of Reference

"MARKET STUDY ON NIS INVESTMENTS"

for ENISA F-COD-20-T23

PLEASE NOTE:

This Scenario Project will result in a specific contract to be awarded concurrently with the 4-year Framework contract to the successful tenderer. Please therefore take all due care to furnish a practical and achievable technical and price offer, as it will be used to commit the winning tenderer to the first contracted project under this framework.

CONTENTS

1. GENERAL DESCRIPTION OF THE REQUIRED SERVICES

1.1 Background Information

Business drivers resulting in a digital transformation in all sectors have brought cybersecurity at the forefront for many organisations. This trend has been enhanced by the continuous development of the relevant EU Regulatory and Policy Framework with the introduction of the Network and Information Security (NIS) Directive[1], the EU Cybersecurity Act[2] and the Digital Single Market Strategy[3] among other initiatives. However, not enough data currently exists in the EU on how this trend has manifested in terms of cybersecurity investments in the private sector.

The Cybersecurity Act provides that "*In order to support the businesses operating in the cybersecurity sector, as well as the users of cybersecurity solutions, ENISA should develop and maintain a 'market observatory' by performing regular analyses and disseminating information on the main trends in the cybersecurity market, on both the demand and supply sides*."[4]

ENISA is looking to contract services that will provide market data and the relevant analysis thereof in relation to how EU operators in different sectors are investing in NIS products and services. ENISA intends to use this data to assess how the budget of private sector operators committed to cybersecurity projects has evolved, what specific aspects of cybersecurity are prioritized in each sector and how are NIS investments expected to evolve in the near future.

The resulting report will be used to help ENISA to develop its role as a market observatory in accordance with Article 8 Market, cybersecurity certification, and standardisation of the Cybersecurity Act and support the drafting of recommendations towards relevant policy makers and inform future policy decisions.

1.2 Objectives

The objective of this project is to support the drafting of a report consolidating a representative sample of market data related to NIS investments by private sector operators in the EU in order to allow for a comprehensive analysis of how the relevant NIS budgets have evolved and what the spending priorities are. In order to meet this primary objective, three project objectives are foreseen:

- Definition of a framework and collection of relevant quantitative and qualitative data related to NIS investments
- Analysis of market data to identify patterns, challenges, gaps etc.
- Drafting of recommendations based on the analysis findings

The contractor is expected to have an existing collection of relevant data and supplement it if necessary in order to support the relevant analysis. The contractor is also expected to have substantial experience in analysing market data, including data related to cybersecurity products and services, in order to support the analysis and validate the adequacy of the available datasets to conduct the analysis.

---

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[3] https://ec.europa.eu/digital-single-market/en

[4] Cyber Security Act, Rec. 42

2. DELIVERABLES AND TASKS

Deliverable

The contractor should produce one deliverable:

- D1: Market study on NIS investments.

This deliverable should consolidate all cybersecurity investment information collected and analysed in order to meet the aforementioned project objectives. In the following paragraphs of this document, we describe the detailed tasks, which will have to be carried out by the tenderer to reach the previously described objectives and generate the deliverable.

We expect the tenderer's offer to include a project plan, along with milestones, dates and intermediate deliverables, as well as a more detailed description of how it intends to approach and carry out each of these tasks, **clearly explaining the type of market data the tenderer can make available in support of the study**.

2.1 Task 1 – Collect data on cybersecurity investments

The objective of this task is to collect, group and present market **quantitative and qualitative data** on private sector cybersecurity investments.

In this task the prospective contractor will work with the ENISA project team to define the framework that will be used to group, present and analyse the relevant market data. The resulting framework should cover the key elements of cybersecurity investments by EU (and non-EU for comparison) private sector operators of different organisation sizes (Large Corporations, SMEs etc.), allowing for comparisons between sectors and/or countries (including EU and non-EU), allowing for a more granular analysis of how cybersecurity budgets are allocated etc.

Emphasis should be placed on the sectors defined in Annex II of the NIS Directive[5] and sectors related to the Cybersecurity Act, covering organisations of different organisation sizes and including SMEs.

The proposed framework should take into consideration the relevant market data readily available to the contractor and can consider elements such as:

1. NIS investment data per sector/country/organisation size/security domain and any relevant combination. With respect to the security domains, a proposal built around the domains of widely accepted industry frameworks such as ISO 27001, COBIT etc. to group the investment data would be preferred;
2. Microeconomic data on NIS investments, such as how much organisations invest as a percentage of their total expenditure or total IT budget;
3. Cybersecurity investment trends, drivers etc.
4. Data on the average cost of security breaches;
5. Investments related to the recruiting of NIS staff;

---

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

The tenderer is expected to propose a preliminary framework in the technical offer specifically mentioning the type of data already available. The proposed framework should also take into consideration how the data will be presented in the final report (e.g. in terms of readability).

The result of this task is a set of figures, graphs, charts etc. presenting the relevant market data in a comprehensive and useful way, which will form the basis for the subsequent analysis.

It is expected that the tenderer will have available datasets to support the consolidation of the required data without necessarily the need to complement the dataset with other sources. In case of the latter, the tenderer should clearly explain in their offer how they intend to obtain any missing market data.

2.2 Task 2 – Analysis of market data

After the collection of the market data on cybersecurity investments and the production of the relevant graphs, charts etc. the contractor will conduct an analysis in order to identify gaps, patterns, challenges, issues, opportunities etc. The contractor should have adequate expertise in analysing market data to identify statistical correlations and important findings to support the analysis. The contractor should also have appropriate understanding of the subject matter in order to support a qualitative analysis of the findings in a methodologically sound way.

The result of this task is a list of key findings resulting from the analysis of the market data on cybersecurity investments.

2.3 Task 3 – Recommendations

Based on the findings resulting from Task 2 the contractor together with ENISA will draft a set of recommendations in order to address the identified challenges and gaps and leverage the identified opportunities. The recommendations will outline potential policy actions.

The result of Task 3 will be the complete deliverable D1, comprising the individual outputs of each task, i.e. the market data, the key findings and the recommendations in a single report.

The report should clearly specify traceable sources for all information and well-reasoned argumentation for any judgements made. It should also clearly separate conclusions from any technical argumentation supporting them. This way the conclusions are understandable by non-technical readers.

If required ENISA will request proof reading services to be provided by a native EN speaker. This will be included in the tasks of the contractor.

2.4 Task (on-going) - Project management

We expect the tenderer to carry out appropriate project management, and to adopt a sound planning of time and resources, according to proven expertise and prior knowledge of the subject.

We expect the tenderer to interact with ENISA staff regularly and to provide progress reports on a regular basis. The tenderer will need to send to ENISA a brief **monthly progress report** explaining the status of tasks in the planning and issues if any. The tenderer is expected to discuss progress with ENISA in a virtual meeting (conference call) on a **bi-weekly** basis and provide the minutes of these calls.

The prospective contractor is expected to submit, prior to the kick off meeting, a detailed Gantt chart, describing the project plan in more detail. These will be discussed with ENISA in the kick-off meeting before confirmed as final.

The Gantt charts and related documentation should include:

- Scheduling of all tasks and activities within objectives and their respective tasks
- Identification of milestones and critical activities
- Identification of possible risks and suggestions to mitigate them
- Quality assurance and peer review measures to ensure high quality results
- Detailed information on the expertise of the prospective contractors on the tasks and topics of this tender including references to previous, relevant projects,
- 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 prospective 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
    - 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 prospective contractor is expected to deliver the following documents regularly:

- Monthly progress report on current activities (as they 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 (bi-weekly or at more frequent intervals to be agreed upon) on the progress achieved.
- Monthly progress reports (template provided by ENISA).
- It is expected that the prospective contractor performs a first level of proof-reading before transmitting any document to ENISA and proof read the final deliverable by an English native speaker prior to submission.

The contractor is expected to send two-weekly progress reports using the ENISA template to the ENISA project manager(s) about the project and to schedule bi-weekly videoconference meetings about the progress.

The progress reports should include (in bullets) what has been done the previous two weeks, the status, what is planned for the next two weeks, the risks and suggested solutions and finally, points to take decisions upon.

After every meeting (progress meetings, or project meetings), the contractor should take minutes and send them to the ENISA project manager(s) using the ENISA template.

3. EXPECTED SKILLS

The performance of the above mentioned tasks requires professionals that have good professional multi-disciplinary knowledge on all or a sub-set of the following fields:

- Excellent knowledge in analysing market data and producing key findings from large datasets.
- Knowledge and experience in the field of network and information security.
- Excellent knowledge of data collection and validation methods including the ability to produce clear and understandable text equipped with graphical elements.
- Familiarity and experience with the tasks performed by ENISA is a plus.
- Policy and regulatory issues related to the resilience of critical infrastructures and services at national and/or European level including activities related to CIIP and National Cybersecurity Strategies.
- Excellent project management skills including quality assurance and risk management and experience in realising international projects.
- Excellent communication and presentation skills.
- Excellent native English proof reading skills.

4. DURATION AND DEADLINES

The duration of this work is foreseen from the mid/late August 2020 until the 27th of November 2020.

- Kick of meeting – no later than 25th August 2020.
- Collection of data and production of graphs – no later than the 30th of September.
- Analysis of data and consolidation of findings – no later than the 30th of October.
- Final draft of the deliverable D1 – no later than the 6th of November.
- Final deliverable D1 – no later than the 20th of November.
- The contractor might need to integrate comments and update the final draft from validations and discussions until the end of the contract (27th of November).

The Tenderer is required to make a proposal in their proposal for the time schedule of the activities in order to carry out the project (e.g. including a Gantt chart). The tenderer may propose to carry different activities in parallel. In its proposal the Tenderer shall indicate the estimated amount of person days required to accomplish all tasks associated with this procurement.

ENISA expects that the contractor will deliver a project plan indicating the execution of these activities.

5. LIST OF DELIVERABLES

The contractor is expected to produce one deliverable:

D1 - the output from the Tasks 1-3 listed above.

English is the language to be used for all the documents produced. The layout of the final report should be based on the templates provided by ENISA. The final report is expected to be proofread by a native English speaker. At the end, ENISA may edit the full report and publish it.

English is the language to be used for all the documents (interim and final reports, project management reports etc.) produced.

The final deliverables should use the standard ENISA document templates, which will be provided to the successful contractor. In addition, final deliverable should be written and proof-read by the Contractor following the European Commission English Style Guide[6] or any other style guide document that ENISA will provide to the successful contractor

6. 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.

At least the following communication with the contractor is expected.

- A physical or virtual kick off meeting at the ENISA Office in Athens
- Regular video or teleconferences on the progress achieved

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.

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

7. ESTIMATED CONTRACT VALUE

The total estimated budget cannot exceed **150,000.00 Euro (one hundred and fifty thousand Euro)** and **not be less than 130.000,00 Euro (one hundred and thirty thousand euro)** covering all tasks executed and including all costs (e.g. travelling expenses of the Contractor to and from ENISA's premises).

8. CONTENT AND PRESENTATION OF THE SCENARIO TECHNICAL OFFER

The Tenderer shall enclose with the **Technical Offer** all documents and information that will enable its offer to be assessed in terms of quality and of compliance with the Scenario Specifications. An Offer shall include a description of the operational means and procedures to be implemented to perform the Contract, supported where appropriate by related documents.

The Technical Offer should be structured as follows:

---

[6] http://ec.europa.eu/translation/english/guidelines/documents/styleguide_english_dgt_en.pdf

- **Section 1: Skills and experience** (20% of total Scenario score)
    - The Tenderer will have to present its **compliance with the expected skills** as described in the relevant section.
    - Examples of previous related works, a **list of all related projects and activities** that the contractor has undertaken in the past, particularly in relation to the collection and analysis of cybersecurity market data.
- **Section 2: Tasks and Deliverables** (40% of total scenario score)
    - A **preliminary proposal for the framework** indicating the type of data the tenderer foresees will be of value to the objectives of the project.
    - A clear indication of the **readily available data** the tenderer can bring to the project. Any case of important data that will need to be obtained during the project must be clearly indicated and the tenderer must explain the process for obtaining it in due time.
    - The description of the **approach and methodology** to perform each task and ensure the quality of the respective output.
- **Section 3: Project Team** (20% of total scenario score)
    - **Short CV's of the experts** that will be allocated in the project focusing on their experience and expertise on the areas covered by the study.
    - Description of relevant **roles/responsibilities** within the proposed project team
    - Description of **tasks/activities** to be undertaken by each project team member
    - **Allocation of person-days** per project team member and per task.
    - If applicable, **justification for subcontracting**
- **Section 4: Project Management and Quality Assurance** (20% of total scenario score)
    - The approach and methodology for overall project management, communication and quality control, including provisions for proof reading of deliverables
    - Project planning, including project Gantt Chart with key milestones
    - The foreseen project risks and how are going to be mitigated.

9. CONTENT AND PRESENTATION OF THE SCENARIO PRICE OFFER

The Scenario Price offer must be drawn up using the Financial Offer template provided (see Annex III).

10. PRICE

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