Scan to verify source & version of document.

OPEN CALL FOR TENDERS

Concluding with:

Multiple Framework contracts with 're-opening of competition'

"Supporting Critical Information Infrastructures Protection activities"

ENISA F-COD-16-T32

Part 1 **Introduction to ENISA**

Part 2 **Terms of Reference**

Part 3 **Tender Specifications**

Annex I	Legal Entity & Financial ID Forms
Annex II	Declaration on honour on exclusion criteria and selection criteria
Annex III	Financial Offer form
Annex IV	Draft Framework Service contract
Annex V	Power of Attorney for Consortium Form
Annex VI	Sub-Contractors Form
Annex VII	Checklist of documents to be submitted in the e-Submission application
Annex VIII	e-Submission Quick Guide for Tenderers
Annex IX	Guide to creating an ECAS account (EU Login)

e-Submission

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

CONTENTS

PART 1 INTRODUCTION TO ENISA

1. Background on ENISA

1.1 Introduction

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

1.2 Scope

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

1.3 Objectives

The Agency's objectives are as follows:

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

2. Additional Information

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

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

PART 2 TERMS OF REFERENCE

I. SCOPE OF THIS TENDER

The purpose of this Call for Tenders is to provide support for the ENISA work in the area of Critical Information Infrastructure Protection (CIIP), throughout the years 2017 - 2018. ENISA envisages around 3 projects per year in this area, on specific topics (for example, baseline security measures for the energy sector, baseline security measures for health sector, identification of dependencies in the healthcare sector, procurement language for the energy sector, identification of criteria for the selection of ESOs under the NIS Directive etc.).

By means of this Call for Tenders ENISA seeks to contract the services of a minimum of two (2) and maximum of five (5) service providers which can provide support in the field of CIIP. The successful bidders should be able to demonstrate significant experience and skills in in the area of CIIP, with emphasis on the aspects dealt with in the annual ENISA work programme (which will be described below).

Subject of the tender	Maximum budget
Supporting Critical Information Infrastructures Protection activities	An estimated budget of **€400,000.00** over the maximum possible period of 2.25 years (15 + 12 months)
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.)*	

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

II. ELECTRONIC SUBMISSION OF OFFERS

*Please see **ANNEX VIII** of this Tender for a quick description of the e-Submission application.*	

Access to the e-Submission application

If you are accessing a tender procedure linked to e-Submission via the e-Tendering platform *for the first time*, you will need to create a user account in the Commission system **European Commission Authentication Service – ECAS** (to be renamed **'EU Login'** as of early October 2016): https://webgate.ec.europa.eu/cas/

A ***'Guide to creating an ECAS account'*** is provided as Annex IX to this Tender.

A button "Submit your Tender" will be then displayed and you will be able to access the e-Submission application.

Before proceeding to fill in the tender details in the system, you need to accept the Terms & Conditions and acknowledge the Privacy Statement of the e-Submission application.

On-time submission of tenders

You are ***strongly advised*** not to wait until the last moment before the deadline to submit your tender. The process of uploading your documents and entering required data may take longer than anticipated.

> ***It is highly recommended to give yourself a MINIMUM of 24 - 48 hours before the stated expiry date and time to upload your tender to e-Submission!***

In case of any problems with the submission of your electronic tender, we recommend that you call the helpdesk in reasonable time before the time limit for receipt.

After submitting a tender, but within the time limit for receipt, you may still submit a new (updated) version of your tender. To do this, you should upload a new consolidated tender package containing corrected tender documents together with formal notification by email that the previous tender is withdrawn (to procurement@enisa.europa.eu).

> ***Late receipt of your tender will lead to its exclusion from the award procedure for this contract.***

Proof of receipt

You will receive a tender receipt confirmation in your e-Submission mailbox, including information about the timestamp put on your tender by the e-Submission system. This is considered as the official time of receipt and will constitute proof of compliance with the tender deadline.

Withdrawal of tender

If, after submission, you wish to withdraw your tender, you must send a duly signed letter, firstly by email to procurement@enisa.europa.eu as well as by registered post to the address below identifying the name and reference of the tender you wish to withdraw. This notification must be signed by the same authorised legal representative(s) who previously signed the tender in question.

Address
[*Insert tender title and reference*]
ENISA
For the attention of the Procurement Officer
PO Box 1309,
Heraklion 710 01,
Greece

Get to know the e-Submission application

On the ***'Help for e-Submission'*** page of the application a detailed *User Manual,* in each of the 24 languages of the European Union, is available that elaborates the system requirements and a step by step procedure to successfully submit a tender.

A ***Quick Guide*** can also be found on this Help page, summarising the User Manual (*the English version is included as Annex VIII of this tender*).

The 'Help for e-Submission' page is available at:
https://webgate.ec.europa.eu/supplier_portal_toolbox/esubmissionFileProject/files/BT3/spotsHelpPage_en.html

TEST environment for e-Submission application

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

Select the first link if the Call for Tenders has NO LOTS, or the second link for a tender with LOTS.

For a tender with **NO** LOTS:
https://webgate.ec.europa.eu/supplier_portal_toolbox/spots/openSpots.do?CFTUUID=TEST_CFT-NO_LOTS&VERSION=1&CAID=5790001791483&screenWidth=1000&screenHeight=850

For a tender **WITH** LOTS:
https://webgate.ec.europa.eu/supplier_portal_toolbox/spots/openSpots.do?CFTUUID=TEST_CFT-3_LOTS_3&VERSION=1&CAID=5790001791483&screenWidth=1000&screenHeight=850

1. EXPLANATION OF 'REOPENING OF COMPETITION' PROCEDURE

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

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

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

e-PRIOR Supplier Portal

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

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

- e-Request
- e-Invoicing

ENISA has implemented the electronic offer submission system called '*e-Request'* specifically for the 'reopening of competition' tender procedures. The resulting framework contractors chosen as a result of this Open tender procedure will therefore be expected to use '*e-Request'* as the sole method for participating in the subsequent 'Request for Offers' procedures.

For more information an FAQ page is available from DG Informatics:

http://ec.europa.eu/dgs/informatics/supplier_portal/faqs/faqs_en.htm

2. BACKGROUND INFORMATION

3.1 ENISA's past work on Critical Information Infrastructure Protection

Previous ENISA work on Critical Infrastructures, ICS-SCADA security and eHealth security:

- Stock Taking of National Policy and Regulatory Environments (2008), aims at identifying at national level all relevant authorities (stakeholders) and focuses on their tasks, existing policy for the resilience of telecommunication networks;
- Analysis of Policies and regulations, Policy Recommendations (2009), analyis of the stock taking input from the 2008 report;
- Inter-X: Resilience of the Internet Interconnection Ecosystem (2010), the resilience of the system of interconnections between Internet networks;
- Resilience of the Internet Interconnection Ecosystem (2011), which looks at the resilience of the Internet interconnection ecosystem;
- National-level Cooperation Plans (2011), guideline in the development process of coordinated response and crisis management of large scale CII incidents;
- Good Practices for Resilient Internet Interconnections (2012), a follow up on the Resilience of the Internet Interconnection Ecosystem study;
- Guidelines for enhancing the Resilience of eCommunication Networks (2013), aiming at understanding the importance of the Internet infrastructure within national borders with particular attention to critical assets and cross border interdependencies;
- Protecting Industrial Control Systems. Recommendations for Europe and Member States (2011), describes the 2011 situation of Industrial Control Systems security and proposes seven recommendations to improve it;
- Good Practices for an EU ICS Testing Coordination Capability (2013) which looks on the status of Testing Labs and standards in Europe and proposes a set of recommadations so to achieve a greater level of coordination in this area;
- Can we learn from SCADA security incidents? (2013) provides recommendations for the implementation of a proactive environment that will facilitate agile and integrated response to incidents and their ex-post analysis;
- Window of exposure… a real problem for SCADA systems? (2013) this is a follow up from previuos reports on " the research in the area of Patching and updating equipment without disruption of service and tools";
- National-level Risk Assessment (2013), understanding of the lifecycle of National NIS Contingency Plans (NCP) lifecycle;
- Methodologies for the identification of Critical Information Infrastructure assets and services (2014), provides an overview of existing approaches in identification of CIIs across Europe; Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors (2015), addresses the current cyber security maturity levels as regards the ICS-SCADA protection in the European Member States; and
- Stocktaking, Analysis and Recommendations on the protection of CIIs (2016), presents the different approaches the EU Member States take to protect their critical information infrastructures.
- Security and Resilience in eHealth Infrastructures and Services (2015), investigates the approaches and measures the MS take to protect critical healthcare systems.

3.2 ENISA's work on supporting the EU CIIP activities

ENISA assists competent national EU agencies, the private sector and EU Commission to develop sound and implementable preparedness, response and recovery strategies, policies and measures that fully meet the emerging threats critical information infrastructures face today.

On March 30 2009, the European Commission adopted a Communication on CIIP, and two years later took stock of the results achieved in the Communication on CIIP on 'Achievements and next steps: towards global cyber-security. In all these documents, the EU considers that ENISA can play a key role at European level in the protection of critical information infrastructure by providing technical expertise to Member States and European Union institutions and bodies, as well as through reports and analyses concerning information system security at European and global level.

In 2013, its Cyber Security Strategy the Commission describes many activities for ENISA:

- Assist the Member States in developing strong national cyber resilience capabilities, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure.
- Launch in 2013 a public-private platform on NIS solutions to develop incentives for the adoption of secure ICT solutions and the take-up of good cybersecurity performance to be applied to ICT products used in Europe.
- Propose in 2014 recommendations to ensure cybersecurity across the ICT value chain, drawing on the work of this platform

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

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

- Assistance for MS and the EU Commission by providing its expertise and advice and by facilitating exchange of best practices.
- Assistance for MS in developing national NIS strategies, a task already started several years ago.
- Participation within the Cooperation Group.
- Support EU Commission in developing security and notification requirements for ESPs and DSPs.

- Assistance for MS in developing national CSIRTs, a process that has been successfully going on for some years now
- Coordination/secretariat/Active Support of the CSIRT network.
- Advices and guidelines regarding standardization in NIS security, together with MS.

In this context ENISA has established many working groups in different areas of interest (i.e. the Smart Infrastructures Security Expert Community (SISEC) with focus on smart grids and smart infrastructures, Internet infrastructure security and resilience reference group (INFRASEC), the ENISA ICS Security Stakeholder Group (EICS-SG) focused on the topic of the ICS SCADA security, seen as an opportunity for ICS/SCADA experts to address important issues to ENISA in its work to enhance ICS security in the EU, the eHealth Security and Resilience experts group).

3. PROJECTS PLANNED FOR 2017

Without this being binding on ENISA, it is envisaged that the following projects based on the 2017 Work Programme in the area of Critical Infrastructure Protection, will be tendered early in 2017 to the successful framework contractors:

- Identification of minimum security measures in the energy sector.
- Identification of minimum security measures in the drinking water sector.
- Identification of baseline security requirements in the healthcare sector.
- Criteria for the identification of essential service operators.

4. AREAS OF EXPERTISE

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

- ICS-SCADA security issues e.g. OT security, IT/OT convergence, large scale scanning (like SHODAN) etc.
- Policy and regulatory issues related to the resilience of critical infrastructures and services as well as ICS-SCADA at national and/or European level including activities related to CIIP and ICS-SCADA security.
- CIIP and cyber security strategy and policy at national and/or European level e.g. the European Critical Infrastructures Directive (2008/114/EC), the European Cyber security strategy
- Essential service (e.g. energy, drinking water) operations and security practices and knowledge of the regulatory framework e.g. NIS Directive, the GDPR, the EU Telecoms Package.
- Incident reporting and relevant incident reporting schemes in critical sectors e.g. telecommunications (articles 13a of the telecom package).
- CIIP good practice guidelines and standards e.g. ENISA good practice guides, CPNI's good practice guidelines to industrial control systems security, ANSSI ICS security documents

(Classification Method and Key Measures" and "Detailed Measures."), IEC 62351. IEC 62443, ISO 27001, ISO 27002, ISO 27019, NERC CIP standards, ANSI/ISA 99 etc.

- Network and information security of eHealth systems, infrastructures and services.
- Policy and regulatory issues related to the resilience of critical infrastructures and services as well as eHealth policies at national and/or European level.
- Security for medical devices, such as mobile devices, wearable devices, implantable devices etc
- Network and information security issues e.g. internet and web security, cryptography, testing, security management etc.
- Infrastructure security and resilience and CIIP issues like Public Key Infrastructures (PKI) and core protocols e.g. BGP, DNS etc.
- Internet operations in network and security management for large network providers and Internet Exchange Points.

5. DESCRIPTION OF TASKS & SERVICES TO BE PROVIDED

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

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

- Update existing inventories, reports, studies, surveys, etc.

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

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

6. POOL OF EXPERTS AND EXPERT PROFILES

The successful tenderers shall have a pool of experts available for individual assignments/tasks. The experts for individual assignments will be selected depending on their availability and experience with regard to the specific requirements related to each project. The pool shall comprise experts of both junior and senior category. You are required to provide only the CVs of experts deemed relevant and experienced on the above-mentioned topics.

For this call in particular, we expect that you should include at least 4 experts; at least 2 ‘Senior Experts’ and at least 2 ‘Junior Experts’ (see below):

6.1 Junior Expert profile

The Junior Expert shall have:

- Minimum 2 years of professional experience in the field of network and information security and/or in CIIP activities and/or ICS-SCADA security and/or medical devices security and/or healthcare systems security;
- Minimum 2 years of prior experience (academic or professional) with technical aspects of CIIP and/or ICS-SCADA security and/or healthcare information systems security or hands-on experience in CIIP and/or ICS-SCADA and/or medical devices security deployment and implementation;
- Very good drafting skills and ability to draft technical reports.
- Excellent communication and presentation skills.
- Proficient in both written and spoken English.

Advantageous:

- Knowledge of EU directives, EU national laws, and international laws concerning network and information security (NIS) and more specifically laws and secondary laws relevant for ICS-SCADA and/or eHealth and/or CIIP;
- Experience in pre-research or in academic research (literature reviews and desk research);
- Interdisciplinary knowledge of areas related to NIS (e.g. social issues, awareness raising, legal issues, etc.);

6.2 Senior Expert profile

The Senior Expert shall have:

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

Advantageous:

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

7. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

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

The Technical Offer shall include the following:

- Presentation of tender proposal;
- Evidence demonstrating expertise in the fields covered by this call for tender;
- Management practices, planning and resource allocation to tasks and experts;
- Project management method that will be used for projects under this framework contract, explaining how possible projects would be carried out efficiently and effectively;
- The procedure for the provision of consultants (e.g., backup solutions etc.);
- In the case of a tender being submitted by a consortium, a description of the input from each of the consortium members and the distribution and interaction of tasks and responsibilities between them;

- A description of sub-contracting arrangements foreseen, if any, with a clear indication of the tasks that will be entrusted to a sub-contractor and the quality assurance methods to be used in relation to these tasks. A statement by the tenderer guaranteeing the eligibility of any sub-contractor shall be included as well, in case the subcontractor/s are not known at the moment of the tender submission.

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

8. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

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

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

These prices must be a flat rate and include all administrative costs, with the exception of reimbursable costs in relation to travel and overnight stays away from your principal place of business if requested as part of the 'Request for offers'. These costs will be reimbursed as follows:

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

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

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

9. TENDER RESULT AND ESTIMATED CONTRACT VALUE

The estimated overall maximum contract value without this being binding for ENISA cannot exceed **four hundred thousand Euros (€ 400,000.00)** over a maximum possible period of 2.25 years (15 + 12 months).

It is important to note that the amounts stated above apply to **all** framework contracts signed under the 'multiple framework contracts' system in total and not for each framework contract. There will be a minimum of two and a maximum of five framework contracts signed, provided that there are a sufficient number of admissible tenderers that meet the award criteria following the evaluation of offers.

(Please note that in the case where unforeseen circumstances result in this contract being consumed faster than originally planned, the Agency reserves the right to consider conducting a 'Negotiated procedure without prior publication of a contract notice' with the existing contractor(s) in order to increase the maximum amount stated above by up to 50%.

This procedure being fully in accordance with Article 134(e) of the Rules of Application (RAP) implementing the EU Financial Regulation (FR)).

10. DATA PROTECTION

Personal contact information will normally be professional contact data only, so no special confidentiality requirements are envisaged.

Regarding personal data, the following EU data protection regulations have to be respected:

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
2. Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;
3. Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

11. MARKING OF SUBMITTED DOCUMENTS

The tenderer SHOULD NOT mark tender documents (for e.g. the header or footer) with any of the following words: RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET. If the tenderer considers that such markings are required, a prior approval from the ENISA Procurement office should be attained BEFORE sending the tender documents. The tenderer should be aware that the information sent to ENISA for procurement purposes is handled in accordance with the governing rules for EU Public Procurement and the EU Financial Regulation framework.

12. PRICE

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

13. PRICE REVISION

Price revision does not apply to this tender procedure.

14. COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER

ENISA will not reimburse any costs incurred in the preparation and submission of a Tender. Any such costs must be paid by the Tenderer.

15. PERIOD OF VALIDITY OF THE TENDER

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

16. PROTOCOL ON PRIVILEGES AND IMMUNITIES OF THE EUROPEAN COMMUNITIES

ENISA is exempt from all taxes and duties, including value added tax (VAT), pursuant to the provisions of Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Communities. Tenderers must therefore give prices which are exclusive of any taxes and duties and must indicate the amount of VAT separately.

17. PAYMENT ARRANGEMENTS

Payments for specific contracts awarded under the Framework Contract (see section 19 below) shall be carried out within 60 days of submission of an invoice accompanying the final report or deliverable based on the conditions set out in the draft contract. One single payment will be made after receipt and approval of the deliverables by ENISA. An invoice must specify the specific deliverables covered. A note that accompanies the final deliverables must present the resources used for each of the deliverables presented. Time sheets should be submitted as appropriate

18. CONTRACTUAL DETAILS

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

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

The tender will conclude, valid as of the date of the last signature, with a 15 month Framework Service contract, tacitly renewable once for a further 12 months - in total a maximum of 2.25 years.

The Agency reserves the right to end the contract at any time, without any obligation to invoke the reason for it, at one months' notice.

The Tenderer's offer must be drafted taking fully into account the provisions of the draft Framework Service contract annexed to this call for tenders (See draft contract, in Annex IV).

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

19. PROVISION OF SERVICES - Re-opening of Competition

At the conclusion of this tender procedure, at least 2 and up to 5 contractors will be awarded multiple framework contracts. These contractors will then be eligible to bid for specific future projects based on the 'Re-opening of Competition' procedure which is explained below:

- ENISA launches a 'Request for Offers' (tender procedure) on a specific subject matter to each of the contractors awarded a framework contract. The offer shall only consist of a technical offer and will not require any administrative paperwork or proof of economic stability to be re-submitted.

- The Framework Contractors respond typically within 7 - 10 working days with a detailed technical offer. This offer will contain all aspects regarding:

    - Technical content relevant to the specific subject matter
    - Experts offered (*they should be from the pool of experts already offered but an alternative can be offered in exceptional circumstances which are well documented*)
    - A project plan
    - Proposed duration of consultancy in person-days
    - Cost

- ENISA will evaluate all offers received by the closing date for reception of offers. A Specific Contract will be awarded to the best offer in terms of the following award criteria:

  Quality:

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

  Price:

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

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

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

For each Specific Contract the contractor will designate a Project Manager. The Project Manager will be responsible for overall management of the assignment, the timely completion of the activities and the quality and timely delivery of technical reports.

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

PART 3 TENDER SPECIFICATIONS

1. INFORMATION ON TENDERING

1.1 Contractual conditions

In drawing up their offer, the tenderer should bear in mind the provisions of the draft contract (Annex IV) attached to this invitation to tender particularly those on payments, performance of the contract, confidentiality, and checks and audits. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein. Any limitation, amendment or denial of the terms of contract will lead to automatic exclusion from the procurement procedure.

It is strongly recommended that you have this draft contract checked and passed by your legal representative before committing to submitting an offer.

The Agency may, before the contract is signed, either 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 sign by all members of the grouping. In this case, one of them will be responsible for the receipt and processing of payments for members of grouping, for managing the service administration and for coordination of the contract; or
- to have the contract sign by a team leader, which has been duly authorised by the other members to bind each of them (a power of attorney 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 discretion.

In case of a joint offer, for each partner, except the LEAD partner:

- the **Legal Entities form** and the **Power of attorney of each partner**, must be filled in, signed by (an) authorised representative(s), scanned and uploaded in the corresponding section.

- the **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.

More details about uploading the respective documents can be found in Annex VII.

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[2] 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, on the grounds that 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, the change of any 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 clear and concise, 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.

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

2.2 Structure of the tender

Based on the *e-Submission* environment, all tenders must include two sections:

1) Qualification data;
2) Tender data.

The 'Qualification data' consists of:
- Identification of the Tenderer;
- The lots the tender is applicable for;
- Information regarding exclusion and selection criteria.

The 'Tender data' consists of:
- The technical proposal;
- The financial proposal.

2.3 Qualification data

a) Identification of the Tenderer

The tenderer must fill in all required fields in the section:
"Qualification" → "Identification of the Tenderer" →"[Party Name]".

In case of a joint tender the consortium name has to be provided in the section:
"Qualification" → "Identification of the Tenderer" →"Consortium"

and an identification of every party in the consortium needs to be added in the section:
"Qualification" → "Identification of the Tenderer" →"Consortium Members".

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'* (see Annex VII for an overview of required signatures.)

However, the subcontractor(s) shall not be required to fill in or provide those documents when the services represent less than 20% of the contract.

The Legal Entity Form can be generated via the e-Submission application from the section:
"Qualification" → "Identification of the Tenderer" → "[Party Name]" → "Documents"

Located under the sub-section:
"Generate pre-filled documents" button "Legal Entity form"

and uploaded under *"Documents"* in the same section.

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 on:
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) 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 section:
"Qualification" -> "Identification of the tenderer" -> "[Party Name]" -> "Documents".
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 of each partner must be filled in, signed by (an) authorised representative(s), scanned and uploaded in section:
"Qualification" -> "Identification of the tenderer" -> "[Party Name]" -> "Documents"

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 boxes in the section:
"Qualification" -> "Interest in the following lots" of the e-Submission application.

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 needs to be uploaded under:

   "Qualification" -> "Exclusion Criteria" -> "[Party name]"

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)

   The documents need to be uploaded under:

   "Qualification" -> "Selection Criteria" -> "Financial and Economic Capacity" -> "[Party name]"

   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)

   The documents need to be uploaded under:

   "Qualification" -> "Selection Criteria" -> "Technical and Professional Capacity" -> "[Party name]"

   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 on the basis of non-conformity with the tender specifications and will not be evaluated.

The technical tender needs to be uploaded in the section:
"Tender" → *"[name of Call for Tender]"* in the e-Submission application.

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 **euros**, including the countries which 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** [and include all expenses, such as travel expenses and daily allowances etc.].

- **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.6 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. The completed Financial Offer form, ALSO needs to be uploaded in section:
"Tender" → "[name of Call for Tender]"

The tenderer selects the "Financial Tender" document from the dropdown box ("Financial Tender or Technical Tender"). The e-Submission application allows attachment of as many documents as necessary.

3. ASSESSMENT AND AWARD OF THE CONTRACT

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

The aim of each of these stages is:

1) to check on the basis of the ***exclusion criteria***, whether tenderers can take part in the tendering procedure;
2) to check on the basis of the ***selection criteria***, the technical and professional capacity and economic and financial capacity of each tenderer;
3) to assess on the basis of the ***award criteria*** each bid which has passed the exclusion and selection stages.

Only tenders meeting the requirements of one step will pass on to the next step

3.1 EXCLUSION CRITERIA

All tenderers shall provide a 'declaration on their honour' (see Annex II), stating that they are not in one of the situations of exclusion listed in Annex II.

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* (see Annex VII for an overview of required signatures.).

The successful tenderer shall be asked to provide the 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:
The tenderers will be waived of the obligation to submit the documentary evidence mentioned above if such evidence has already been submitted for the purposes of another procurement procedure launched by ENISA, provided that the documents are not more than one year old starting from their issuing date and that they are still valid. In such a case, the tenderer shall declare on his honour that the documentary evidence has already been provided in a previous procurement procedure, specifying the reference of the call for tender for which the documents have been provided, and confirm that no changes in their situation has occurred.

3.2 SELECTION CRITERIA

The following criteria will be used to select the Tenderers. If the Tender is proposed by a consortium these criteria must be fulfilled by each partner.

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, in the country of establishment.

3.2.2 Financial and Economic Capacity

Proof of financial and economic standing shall be furnished by the following documents and minimum requirements:

(a) Copy of the financial statements (balance sheets and profit and loss accounts) for the last two (2) financial years for which accounts have been closed, where publication of the accounts is required under the company law of the country in which the economic operator is established. In case of a consortium, each consortium member shall present their financial statements.

If the tenderer is not obliged to publish its accounts under the law of the state in which it is established, a copy of audited accounts for the last two (2) financial years should be presented. In case of a consortium/grouping, audited accounts for each consortium partner shall be presented.

(b) A statement of the average turnover of the last two (2) financial years for which accounts have been closed. The **minimum annual <u>average</u> turnover** of the tenderer shall be of **50,000.00 EUR**. In case of a consortium/grouping, the annual average turnover for each of the partners shall be presented. The sum of the annual average turnovers of each partner will be taken into account to reach the annual average turnover of 50,000.00 EUR.

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 request for clarification <u>before</u> the tender expiry date.

3.2.3 Technical and professional capacity criteria and evidence

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

a) Criteria relating to tenderers

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

- The tenderer must prove its experience in the field of Network Information Security (NIS) related to CIIP and ICS-SCADA security or eHealth security with at least three (3) projects/deliverables delivered in these fields in the last three years, each with a minimum value of € 20,000.00.
- The tenderer must prove experience of working and drafting reports in the English language with at least three (3) projects delivered in this field in the last five years, showing the necessary language coverage.
- The tenderer must prove its experience of working in EU countries with at least 2 projects delivered in the last three years.

- The tenderer must prove experience in one or more of the following as deemed relevant to the area of expertise the subject of this tender; survey techniques, data collection, statistical analyses and drafting reports and recommendations.

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

b) Criteria relating to the team delivering the service:

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

Junior Expert profiles

As per minimum requirements listed in Part 2 section 6.1

Senior Expert profiles

As per minimum requirements listed in Part 2 section 6.2

c) Evidence:

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

- Details of the structure of the organisation
- List of services (relevant to the area of CIIP services) provided in the past five years, with sums, dates and recipients, public or private.
- The educational and professional qualifications of the experts who will provide the services for this tender (CVs), including the management staff. Each CV provided should indicate their intended function in the delivery of the service.

3.3. AWARD CRITERIA

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 on the basis of the award criteria.

No	Qualitative award criteria		Weighting (max. points)
1.	**Rationale, Organisation and Methodology**	Understanding of Terms of Reference, approach, completeness, clarity, methodology, processes, list of activities	35/100
2.	**Relevant experience**	Operational knowledge of the EU landscape related to CIIP security activities	35/100
3.	**Quality control measures**	This criterion will assess the quality control system applied to the service foreseen in this Terms of Reference concerning the quality of the deliverables, the language quality check, and continuity of the service in case of absence of a member of the team.	30/100
Total Qualitative Points (QP)			**100**

Minimum attainment per criterion

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

Minimum attainment overall

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

The sum of all criteria gives a total of 100 points. The respective weighting between the different award criteria depends on the nature of the services required and is consequently closely related to the terms of reference. The award criteria are thus quantified parameters that the offer should comply with. The **qualitative award criteria** points will be weighted at **70%** in relation to the price.

3.3.2 Price of the Offer

The Financial Offer form (Annex IV) contains four (4) price boxes which shall be completed with a monetary amount by the tenderer.

P_S = **(P1 + P2)** will then be used in the price formula as shown below
P_J = **(P3 + P4)** will then be used in the price formula as shown below

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

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

Senior Experts price	70 %
Junior Experts price	30 %

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

where

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

C - is the best price of all bidders for person/day rates for Junior Expert
P_J - is the price for a single bidder for person/day rates for Junior Expert

3.3.3 Award of the contract

The contract will be awarded to the offer which is the most cost effective (offers the best value for money) which obtains the highest number of points after the final evaluation on the basis of 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 **7th November 2016 at 11:00 EET Eastern European (Greek) time** at ENISA Athens office, 1 Vasilissis Sofias Street, Maroussi 151 24 Attiki, Greece.

A maximum of one legal representative per participating tenderer may attend the opening session. Tenderers shall inform the Agency in writing of their intention to attend by email to procurement@enisa.europa.eu **at least 3 working days** prior to the opening session.

5. OTHER CONDITIONS

5.1 Validity

Period of validity of the Tender: 90 days from the closing date stated in Invitation to Tender. The successful Tenderer must maintain its Offer for a further 120 days from the notification of the award.

5.2 Lots

This Tender is not divided into Lots.

5.3 Additional Provisions

- Changes to tenders will be accepted only if they are received on or before the final date and time set for the receipt of tenders.
- Expenses incurred in respect of the preparation and presentation of tenders cannot be refunded.
- No information of any kind will be given on the state of progress with regard to the evaluation of tenders.
- All documents submitted by Tenderers will become property of ENISA and will be regarded as confidential.

5.4 No obligation to award the contract

Initiation of a tendering procedure imposes no obligation on ENISA to award the contract. Should the invitation to tender cover several items or lots, ENISA reserves the right to award a contract for only some of them. ENISA shall not be liable for any compensation with respect to Tenderers who's Tenders have not been accepted. Nor shall it be so liable if it decides not to award the contract.

6. SPECIFIC INFORMATION

6.1 Timetable

The timetable for this tender and the resulting contract is as follows:

Title: **"Supporting Critical Information Infrastructures Protection activities"**

ENISA F-COD-16-T32

Summary timetable comments

Launch of tender: Contract notice to the Official Journal of the European Union (OJEU) Uploaded to e-Tendering website Uploaded to ENISA website	**23rd September 2016**	
Deadline for request of information to ENISA	26th October 2016	
Last date on which clarifications are issued by ENISA	27th October 2016	
Deadline for **electronic reception** of offers via ***e-Submission***	**4th November 2016**	**18:00 CET** **Central** European time
Opening of offers	7th November 2016	**11:00 EET** **Eastern** European (Greek) time
Date for evaluation of offers	TBA	TBA
Notification of award to the selected candidate + 10 day standstill period commences	Mid November 2016	Estimated
Contract signature	Early December 2016	Estimated
Commencement date of activities	As per tender	Estimated
Completion date of activities	As per tender	Estimated