OPEN CALL FOR TENDERS

Tender Documentation

"Web Hosting and (Plone) Web Development services"

ENISA F-COD-20-T18

Part 1 **Introduction to ENISA**

Part 2 **Technical Specifications**

Part 3 **Tender Specifications**

Annex A Service Level Requirements

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 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

I. SCOPE OF THIS TENDER

ENISA would like to find a suitably qualified contractor to provide dedicated (Plone) Web Development and Web Hosting services for ENISA's main website and several ENISA portal sites as stipulated in the Technical Specification outlined below.

ENISA uses various digital communication channels. The ENISA website is an important communication tool to get its message across to government organizations, businesses and citizens across Europe. The scope of this tender includes ENISA's main website (www.enisa.europa.eu) and several ENISA portal sites, i.e. extranets dedicated to specific user groups (for example, working groups, groups of stakeholders, etc.) collaborating with ENISA.

Both the website and the portals are based on the Plone Content Management System; therefore, prospective tenderers shall demonstrate experience and have in-depth knowledge of CMS platforms and Plone in particular. Given the nature of ENISA's work and focus on cyber security, the security of the websites is crucial and so security should receive maximum attention).

Subject of the tender	Maximum budget
Web Hosting and (Plone) Web Development services	A maximum budget of **€950.000,00 (nine hundred and fifty thousand euro)** over the maximum possible period of 4 years. **PLEASE NOTE:** *Out of the overall budget of EUR. 950.000,00 a **maximum of €150,000.00** can be attributed to '**'Web hosting services''** over the maximum possible period of 4 years – including the costs of the one-off 'Migration'*
Last date and time for dispatch of offers	**22nd June 2020 until 18:00 CEST**
***PLEASE NOTE:** This tender procedure is limited to tenderers which are legally incorporated in a member state of the European Union/EEA, or which have an incorporated subsidiary in one of the EU/EEA member states. (The Agreement on Government Procurement (GPA) does not apply to EU Regulatory Agencies.)* **IMPORTANT! Provisions relating to BREXIT** *For UK candidates or tenderers: Please be aware that following the entry into force of the EU-UK Withdrawal Agreement[1] 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.*	

[1] Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community

1. OVERVIEW OF CURRENT ENISA IMPLEMENTATION

1.1 Domain, subdomain and URL structure

The main ENISA website is at https://www.enisa.europa.eu which is a Plone CMS instance.

On a separate webserver there are two portal sites. These two Plone CMS instances are reachable via https://mbportal.enisa.europa.eu, and https://resilience.enisa.europa.eu. The former is referred as 'the management board portal' and the latter as 'the exercises portal' or the 'resilience portal'.

There are also seven websites dedicated to various ENISA's activities. An event website dedicated to ENISA's Annual Privacy Forum https://privacyforum.eu/ is based on Naaya CMS.

The websites and portals are accessible via IPv6 and IPv4 and use mostly HTTPS.

https://enisa.europa.eu

https://mbportal.enisa.europa.eu

https://resilience.enisa.europa.eu

https://www.ecsc.eu

https://privacyforum.eu

https://cybersecuritymonth.eu

https://<new_certification_portal>.enisa.europa.eu

https://<EU Cyber Challenge platform>.enisa.europa.eu

https://www.csirtnetwork.eu.

1.2 Hardware infrastructure

ENISA is currently implementing an infrastructure of two host servers responsible for the production service.

Each of them has the following architecture:

- 2 x 16 Core 3.0Ghz, 155W, 64bit Processors
- 128 GB DDR4 RAM
- 4 x SSD 2 TB
- 2 x Quad Gigabit LAN
- 1000W Redundant (1+1) Power Supplies

The contractor's hosting proposal must provide similar or better hardware infrastructure for the production service and adequate infrastructure for the development and test sites.

It is fully expected that additional equipment will be necessary for backing up the production system's data and settings (See section 2.5).

1.3 Required Technologies

The website and portal servers are built using the following technologies:

Web application firewall:

- FORTINET Web Application Firewall – FortiWeb 400D

Virtualization:

- KVM virtualisation

Operating system:

- CentOS Linux release 7.7.1908 (Core)

Applications layer specific technologies:

- Monitoring service nrpe (client for Icinga2 monitoring system)
- Zope
- Amavis and camb deamon as antivirus for uploaded files
- ZEO database
- Apache/ (CentOS)
- Matomo analytics platform
- Maria DB for Matomo
- Docker server / containers (happroxy, Zeo, Zope)
- Plone built on top of the Zope application server
- ZODB, database used by Zope

2. SERVICE REQUIREMENTS FOR WEB HOSTING

Minimum service requirements regarding the web hosting services are defined in this section. The tenderer shall elaborate in its proposal how each of these requirements will be implemented.

Important notice: Hosting services are restricted to the European Union/EEA area and **must not** be transferred outside the EU/EEA (Including backup datacentre or storage of backup data). Offers that include hosting solutions outside the European Union/EEA will be rejected. Any processing of personal data in the context of the contract shall comply will Regulation (EU) 2018/1725, and in accordance with the provisions of Section 17 of this tender.

2.1 GENERAL CONDITIONS FOR THE PROVISION OF SERVICES

The nature of the service requested will be described in this section. They shall be understood as the minimum service requirements.

The tenderer is allowed to propose additional or higher level service requirements in their offer. In this case, should the proposal be accepted, the tenderer will be bound to its proposal of higher service levels (and the tenderer cannot afterwards refer to the minimum requirements as set out in this section).

We allow proposals including alternative solutions to any of the detailed technical requirements presented in this tender, provided that the tenderer explains that this variation would yield at least a comparable service level.

2.2 WEB HOSTING

The tenderer shall provide hosting services. The tenderer may offer web hosting via a sub-contractor. The proposal should be clear as to which services are being sub-contracted. As a minimum, the following should be provided:

- At least two physical servers for the production website of the specifications as in 1.2 - 1.3 or better
- Servers should have streaming audio and video capabilities;
- Dual connection to a major internet backbone;
- Adequate physical and environmental protection of the servers, and the software and data on these servers, such as fire detection, automatic fire extinguishers, burglary alarms or guards;
- Adequate (logical) access control mechanisms to prevent unauthorized access;
- Adequate security measures to address and prevent cyber-attacks, such as for example, firewalls, intrusion detection systems, anomaly detection, DoS protection, application level protection etc.;
- Adequate screening of staff (security clearances, background checks, - where relevant) and adequate training of staff;
- Redundant physical infrastructure to allow for business continuity (minimum downtime) in case of memory, disk, cpu or power supply failure;
- Redundant physical infrastructure to allow for business continuity in the face of local natural disaster (floods, power cuts, fire, etc.). In other words, a second, physically distant, site should be in use or available in case of need. It should be possible to restore backups in such a way that in case of a disaster the website and portals can be restored online within 24 hours;
- Daily backups of the infrastructure to cater for a restore to a point in time; at most 24 hours in the past;
- 24/7 support to respond to critical issues with the webhosting environment.

Recognised information security accreditations for the organization (or for the sub-contractor that would provide the hosting services), such as ISO/IEC 27001:2013, are preferred. In this case, the proposal shall enclose a certificate from a third-party auditor indicating compliance with the standard practices.

The technical details of the hosting services provided shall be elaborated in the tenderer's proposal and in particular the above-mentioned topics should be addressed.

Whether or not the web hosting is provided in-house or outsourced, the relevant profile(s), for instance the System Administrator, shall be provided. A detailed description of the company which will undertake the web hosting, is required in case it is outsourced

2.3 PRODUCTION AND ACCEPTANCE TEST ENVIRONMENTS

The contractor shall provide two separate environments: a production environment (referred to as P) and a test environment (referred to as T). The tenderer is responsible for making sure that the two environments are identical in terms of software and hardware. In case of real data use on the test environments the security requirements of the test environments are exactly the same as the production environment.

The test environment will be used by ENISA to check and test new developments, changes and bug fixes before deploying them in the production environment. The test environment will also be used by ENISA to run intrusive tests, like vulnerability scans, and performance/load tests.

Logical access to the test environment should be restricted to designated IP addresses

2.4 AVAILABILITY AND RESPONSE TIME

Below we define the minimum service levels for availability and response time: (*see also Annex A: SLR*)

- A minimum availability of 99.0 % must be guaranteed. Availability is to be measured monthly as the number of total available hours divided by the measurement period.
- Planned downtime must be agreed with the Agency at least 3 days prior to the scheduled date, and should be scheduled between 2000 CET and 0600 CET. Planned downtime should not exceed two hours per month. For urgent cases, direct contact with ENISA must be made via telephone to the assigned ENISA contact person (or his/her backup) beforehand.
- Average server response time should be less than 1 second (first byte). Average network time should be less or equal to 3 seconds.

The contractor shall measure and report about availability and response times (see Monitoring and reporting). The measurement of response time should be done in such a way that measurement is representative for normal usage, for example using a probe located in another city or country. Measurements should reveal the average response time

The contractor shall report about these measurements in the monthly reports (*see section 2.8 Monitoring and reporting*).

2.5 BACKUPS

Below we define the minimum backup requirements.

- Daily backups must be made and kept for 8 days.
- Weekly backups must be made and kept for 35 days.
- Monthly backups must be made and kept for 6 months.

- Backup restore requests should be handled within a maximum of 12 hours.

Medium to be used: Discs

The contractor should test backups regularly by testing the backup restore procedure. The contractor should report about success or failure of these tests in monthly reports (*see section 2.8 Monitoring and reporting*).

2.6 PATCHING AND UPDATES OF SERVERS

The requirements around patching and updates of servers are described below.

Critical OS/Server/Application updates and security patches must be deployed within 12 hours of their public release. Normal updates to be performed on a weekly basis. ENISA should be notified prior to each update or patch and all patches and updates should be tested first on a testing environment and then deployed to production.

It is foreseen that the prospective contractor will update on a regular basis outdated libraries and dependencies used by the websites and portals (e.g. JavaScript libraries).

The contractor should report about deployed updates and patches in the monthly reports (*see section 2.8 Monitoring and reporting*).

2.7 TESTING AND SCANNING

Below we define the requirements around testing and scanning:

- The contractor shall periodically test for dead links across the website and portals;
- The contractor shall carry out vulnerability scans periodically, to identify software vulnerabilities in the deployed operating systems or applications. The results of these scans must be reported to ENISA within 5 working days. Serious vulnerabilities should be reported to ENISA immediately;
- Independent vulnerability scans will be performed by ENISA annually in consultation with the contractor;
- The contractor shall perform load or performance tests periodically.

The contractor shall report about the results of these tests and scans in the monthly reports *(see section 2.8 Monitoring and reporting)*.

ENISA can also perform penetrations tests at a given and predefined time after notifying the contractor. With the penetration testing ENISA will evaluate the security of the IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, service and application flaws, improper configurations etc.

2.8 MONITORING AND REPORTING

The contractor shall monitor service levels continuously (*see also Annex A – SLR*) and report about them monthly. The service level reports should address the following items – for the website and the portals separately:

- Overall availability;

- Average response time during the day (hourly averages);
- Average response time per day;
- 404 responses (page not found) per day;
- Number of page hits per day;
- Tests;
- Dead links;
- Security scan results;
- Load test results;
- Backups restore test results

Alternatively, the tenderer could offer a dashboard, instead of using monthly reports.

3. SERVICE REQUIREMENTS FOR WEB DEVELOPMENT

Web development will be requested on a case-by-case basis with requests varying from simple bug fixing, small tasks and enhancements to major web development projects. The contractor shall identify and shall apply appropriate modern technologies and techniques for the web development that will improve and optimize overall, all web-based products of ENISA.

ENISA will provide a functional or technical specification of a new development, new project or a simple change needed and the methodology to be followed will be decided on a case-by-case basis. All basic information, requirements and basic business case will be included as part of the functional specifications sent to the service provider. In each case and depending on the overall complexity of the project, ENISA will provide the service provider, with the project's overall scope, UI general requirements, desired functions, tentative timeline (and required delivery deadline –when relevant)

Web development projects (requests for proposal)

Taking into consideration the complexity of the project, the contractor is expected to provide a preliminary business analysis, a risk assessment, a project plan and a quotation of the amount of work needed (in person hours), a timeline for delivery, and the total costs.

Analysis of business requirements and transposition to technical requirements of most complex tasks/projects (i.e. production of a new tool/web application/website), workflows and wireframes are expected to be done by the contractor as part of the overall web development project. The contractor is also expected to share its expertise on the analysis phase with ENISA project managers in order to facilitate the whole project management flow and assure the end result will reflect all the needs ENISA has on business level. A section that identifies project risks must always be included in the analysis of the contractor at the initial stage.

3.1 DESCRIPTION OF TASKS (WEB DEVELOPMENT PROJECTS)

The contractor will need to perform a number of tasks towards the delivery of each major development (i.e. production of a new tool/web application/website). In this section, a short description of the tasks can be found.

During the project initiation, the contractor will be asked to provide a detailed project plan together with a relevant timeline of the project flow (e.g. Gantt chart) and key milestones that will be agreed with ENISA. Project management methodology (i.e. waterfall or agile methodology) should be the point of reference for all major web development projects. The methodology to be used in each project will be defined by the project manager of ENISA and the contractor should be able to follow both methodologies. Depending on the complexity of the project, all steps of project management shall be followed including validation checks and all have to be applied in every major project depending on the project management methodology.

To this end, the activities mentioned in this section contain an indicative framework for the entire project and will be refined during the project, when deemed necessary.

- **Activity 1**: Set up the project scope
- **Activity 2**: Develop interaction model for the web application/tool – including the development of wireframes/mock ups.
- **Activity 3:** Development of necessary functions
- **Activity 4:** Testing (functional and non-functional)
- **Activity 5:** Deployment
- **Activity 6:** Documentation
- **On-going Activity:** Project Management

In parallel, ENISA will make sure to provide crucial deliverables, feedback, and other necessary information on time for the delivery of web development projects/tasks or to inform the service provider in case of delays.

3.2 SECURITY BY DESIGN

Given the nature of the agency's work/focus, it is of paramount importance that ENISA's environment remains as secure as possible at all times. Security mechanisms, secure functions and security good practices in both coding, configurations and connections shall be utilised to ensure application level security. Corresponding safeguards, e.g. SSL certificates, ISO27001 compliance, etc. shall be considered an advantage.

3.3 COMPATIBILITY

Web development shall always apply cross-platform and responsive design, meaning that all ENISA websites and web apps are mobile friendly. The contractor shall use all cutting edge frameworks or boilerplates to satisfy that need and provide always web solutions that reflect the current trends.

The successful contractor shall ensure and monitor that the website, portals and tools are accessible from (at least) the top five desktop and mobile browsers and applications. Requirements set in section 2. refer to all these browsers and applications.

Service requirements specified in Section 3 shall be met by the contractor wherever applicable to web development and software, e.g. patching, backups, testing and scanning, monitoring and reporting, availability and response time.

4. SKILLS OF WEB-DEVELOPERS

The website and portals currently use Plone, Zope, Apache, Varnish, and Pound Load balancer. The tenderer shall demonstrate experience in these tools and applications. ENISA may want to explore the possibility of using another Content Management System (e.g. Drupal, WordPress) so additional experience with other (widely used) platforms will be considered advantageous.

For the performance of the above-mentioned activities, the following skills and experience shall be demonstrated by the tenderer in the submitted proposal:

- Proven expertise and experience in programming Python, HTML and JavaScript;
- Proven skills in creative development of interactive interfaces covering end-user accessibility and functionality requirements in an attractive/innovative manner (user experience);
- Proven experience in transforming user requirements into demonstrable prototypes;
- Experience in systems integration, availability and security of web and mobile infrastructures;
- Experience in testing, optimization and secure software development;
- Experience in automation tools (eg. automated testing, automated deployment) and scripting languages (eg. bash, perl, python);
- Experience in relevant tasks in both the private and public sector;
- Good project management, interpersonal and coordination skills;
- Excellent command of written and spoken English.

Proven expertise and experience in programming PHP, SQL and NoSQL and using Wordpress API and Codex and/or Drupal API will be considered advantageous.

5. DESCRIPTION OF PROFILES

The tenderer shall be able to provide the following requested profiles for web development services. Whilst not mandatory, any additional profiles provided which are not at the levels suggested below will be evaluated and points will be awarded accordingly.

Note: It is acceptable that one team member might cover two roles provided that this member's profile is at the levels described in this section for both roles and there is no overlap in the tasks (e.g. the developer cannot be the same person as the tester).

5.1 PROJECT MANAGER

Nature of the tasks	• Project management including proposals for project strategies, planning, definition of tasks and deliverables, review of project deliverables, quality control, risk analysis and management, project status reports, problem reporting and management systems, follow up and organisation. • Provide effective leadership for the project team ensuring that team members are motivated and constantly developing their skills and experience. Be in-charge of project activities and review deliverables. • Participate in functional and technical working groups and progress meetings. • Estimate and monitor costs, timescales and resource requirements for the successful completion of each project to agreed terms of reference. • Prepare and maintain project and quality plans and tracks activities against the plan, provide regular and accurate reports.
Education & Experience	• A level of education which corresponds to completed university studies of at least four (4) years attested by a diploma • Minimum 4 years' experience in IT Project Management. Practical experience with software development life-cycle. • Proven experience with quality procedures.
Knowledge and skills	• Project management and leadership. • Usage of project management office tools (e.g. Asana, Atlassian / Jira, MS Project or equivalent). • In depth technical knowledge of the project's main aspects and general technical knowledge on the other aspects touched by the project. • Usage of methods and techniques for reporting. • Ability to give presentations. • Participate in meetings and give status report presentations, be a good communicator. • Capability of integration in an international/multi-cultural environment. • Written and oral English at European language level B2 or better.

5.2 BUSINESS ANALYST

Nature of the tasks	• Liaise with business managers and end-users to understand and document business requirements • Analyse requirements and transform them into technical specifications • Consultancy studies in a specific technical domain regarding information systems. • Production of use case models, software architecture documentation. • Provide expertise in a specific technical domain regarding information systems. • Technical evaluations and provide expertise on integration of IS into the working environment. • Able to draft all the required documentation.
Education & Experience	• A level of education which corresponds to completed university studies of at least four (4) years attested by a diploma in one of the following fields: Computer Science, Information Technologies, Mathematics, Physics, Engineering, Business Administration, Business Management or related areas. • A minimum of four (4) years of experience in Information Technology development and/or Information Technology consulting. • Experience with business process analysis, documentation, and change management as well as experience in working with Plone-related methodologies and technologies • Experience in analysis and programming, databases and web application development.
Knowledge and skills	• Knowledge of international standards like W3C, WAI and IPG(desirable) standards • Conceptual understanding of content structuring, storage, access and presentation elements • Strong interest in follow-up of trends in web development • Ability to participate in multi-lingual meetings • Good communicator • Written and oral English at European language level B2 or better

5.3 DEVELOPER

Nature of the tasks	• Development of web-enabled applications. • Creating/maintaining web applications. • Development of front-end and back-end systems including database development tasks • Develop both simple and complex solutions. • Translate software requirements into concise and robust programming code. • Increase program operating efficiency and adapt system to new requirements, as necessary. • Report status and flag issues to the ENISA Project/Product Manager.
Education & Experience	• University degree in computer science, mathematics, engineering, physics or similar; alternatively, post-secondary degree plus five (5) years proven experience in IT and software development technologies. • At least five (5) years of experience for senior developers and three (3) years of experience for junior developers, developing in a web environment working with python and PLONE – related technologies.
Knowledge and skills	• Top-notch programming skills and in-depth knowledge of modern HTML/CSS • Extensive knowledge of Python, HTML, Javascript and PLONE related technologies (including ZODB) • Experience with version control systems and source code management system for software development, git (preferred) or svn. • Strong interest in follow-up of trends in web development. • Basic knowledge of Search Engine Optimization process • Written and oral English at European language level B2 or better.

5.4 GRAPHICAL INTERFACE DESIGNER

Nature of the tasks	• Definition and creation of the graphical layout of web pages, prototyping. • Collaborate with ENISA project manager and software and website developers to define and implement innovative solutions • Execute all visual design stages from concept to final hand-off to ENISA • Conceptualize original ideas that bring simplicity and user friendliness to complex design roadblocks • Create wireframes, storyboards, user flows, process flows and site maps to effectively communicate interaction and design ideas • Conduct user research and evaluate user feedback • Establish and promote design guidelines, best practices and standards
Education & Experience	• Course on web design at University, or at a specialized institute/school followed by 3 years of experience. • Minimum 3 years of experience in the above tasks. • BS/MS in Human-Computer Interaction, Interaction Design, or related will be considered advantageous • Experience working in an Agile/Scrum development process
Knowledge and skills	• Up-to-date with the latest UI trends, techniques, and technologies • Knowledge of international standards like W3C, WAI and IPG(desirable) standards • Demonstrable UI design skills with a strong portfolio • Solid experience in creating wireframes, storyboards, user flows, process flows and site maps • Proficiency in HTML, CSS, and JavaScript for rapid prototyping. • Excellent visual design skills with sensitivity to user-system interaction • Experience in creating vector graphic images –svgs (desirable) • Written and oral English at European language level B2 or better.

5.5 QUALITY ASSURANCE/ TESTER/ DEVOPS

Nature of the tasks	• Analysis, design, planning and execution of a test strategy for new features and sustaining projects. • Developing and executing automated tests to enable delivery of high-quality software on time and on budget. • Performing functional and non-functional tests in order to ensure the quality and the proper goal of the end product / feature. • Implement test tools and utilities to improve the efficiency and effectiveness of the development life-cycle • Configuration and maintenance of a test lab environment that resembles complex customer environments • File detailed bug reports and follow up on the problems until complete resolution • Comply with good engineering practices, coding standards and contribute to automation code reviews • Collaboration with development team to assure correct replication, integration and deployment on production.
Education & Experience	• University degree in computer science, mathematics, engineering, physics or similar; alternatively, post-secondary degree plus five (5) years proven experience in IT and software development technologies. • At least three (3) years of experience developing/testing in a web environment working with PLONE – related technologies.
Knowledge and skills	• Extensive knowledge of Python, HTML, Javascript and PLONE related technologies • Experience with a Test Automation Framework (e.g. Selenium, QTP, Sikuli) • Experience with QA methodologies • Great understanding of testing throughout the product lifecycle, including unit, integration, regression, component and end-to-end system testing • Familiarity with SSH, and one of the following deployment automation tools (Jira/Bamboo, Jira/Zephyr, Chef, Puppet, Maven, Jenkins, Kubernetes, Capistrano etc.) • Strong scripting programming knowledge (e.g. Shell/Ruby/Python) • Strong system administration knowledge of Linux platforms. • Experience with version control systems and source code management system for software development, git (preferred) or svn.

The **minimum** number of CVs requested per profile is presented below:

ID	Profile	
1	Project Manager	2 CVs
2	Business Analyst	1 CV
3	Developer*	5 CVs
4	Graphical Interface Designer	2 CVs
5	Quality Assurance/Tester/DevOps	2 CVs

*****At least three of the five 'Developers' should be at a senior level, i.e. more than 5 years of experience in web development and database experience, as well as in working with python and Plone-related technologies.

All key roles/resources needed for a project lifecycle shall be used in a web development project to assure quality of end-result (e.g. analyst, designer, developer, tester, pm, etc.). In each phase of the project, the participation in meetings and interaction of the corresponding key expert with ENISA personnel is expected. However not all the roles/resources are needed for helpdesk support and smaller basic tasks and enhancements of the website and portals. The contractor should be able to propose the relevant team members based on the project's/task's requirements.

In case of the departure of one or more members of the proposed team, the contractor is expected to provide ENISA with CVs of replacements with at least the same level of qualifications and similar experience to cover ENISA's needs. ENISA will evaluate the CV and experience in order to decide within 5 working days, whether to accept, or reject and request an alternate replacement candidate.

6. SOFTWARE DEVELOPMENT

Software development shall be documented and new code, or new features shall be deployed first in the test environment.

On a case by case basis (e.g. for the production of a new tool or an enhancement of existing complex applications) automatic testing of the newly developed code will be required by ENISA. The contractor shall be in place to propose the relevant tools for automatic testing, set them up at the beginning of the contract (or when required) and operate them to ensure the overall code quality and performance.

Testing of the overall code performance shall also take place at least annually as an additional exercise and the output should be reported to ENISA.

The contractor is also expected to make sure that the documentation of functionality of the website is always updated.

Access to the code, databases and Version Control System (e.g. git) of ENISA's projects shall be granted to ENISA upon request. ENISA can also perform penetrations tests at a given and predefined time after notifying the contractor.

7. ISSUE TRACKER –TICKETING SYSTEM

The use of Order Forms will be periodically issued for general development services (e.g. bug fixing, small updates) or for new development projects. Within this legal framework, the contractor is expected to operate a ticketing system (such as redmine, flow etc.) to register bug reports, change requests, requests for information, and so on.

Each ticket, together with approval provided by the ENISA responsible person, shall be referred to in the ensuing invoice, which may be partly or fully issued against the amount of the Order, depending on the mutually agreed periodicity of the invoicing.

The tenderer is free to suggest a regular invoicing period, however the Agency would suggest either bi-monthly or quarterly invoicing, in order to reduce administrative burden on both sides

8. BUGS AND ISSUE REPORTS

The contractor shall respond to bug and issue reports based on their classification as per the following table:

Critical: With descending priority, attacks, security updates, website and portals availability, a critical service of the website/portal (e.g. Submission with deadline, such as procurement and recruitment or submission of incident report on incident reporting period) – immediate response (within 2 hours)

High: an issue that prevents an application from meeting requirements or carrying out a feature – response within the same day

Normal: a minor defect that it has no direct effect on the general functionality of the application itself – response within the next 2 days

Low: bugs/issues with no real impact on the functionality of an application (design or cosmetic errors – response within 3 days.

The specific response time per category is further defined in the Service Level Requirements (SLR) which will be annexed to the resulting Framework contract - *see Annex A*.

9. REQUESTS FOR CHANGES

The contractor shall respond to change requests (small enhancements, change of behaviour) at the latest within 3 working days. Request for changes will be reported and monitored using the dedicated ticketing system. The specific response time per type of request or incident is further defined in the Service Level Requirements (SLR) according to the urgency of the latter - *see Annex A.*

10. REQUESTS FOR INFORMATION AND CONSULTANCY

The contractor may be asked to provide consultancy services on the feasibility of implementing various ideas put forward by the ENISA staff. The contractor should respond to requests for information within 5 working days

11. DESIGN AND WEBSITE STRUCTURE

The contractor may be asked to provide advice and technical support in improving the Information Architecture of ENISA's website and portals. The contractor should have (or collaborate with) skilled designers, architects and web usability experts to respond to such requests.

ENISA always seeks to improve the website's information structure and design. It would therefore be considered advantageous if tenderers are able to demonstrate expertise in this respect

12. MIGRATION AND TRANSITION

The contractor is required to migrate the website and portals from the existing hosting environment to the new environment. It is expected that this migration should not take longer than one month.

- The tenderer shall provide a one-off costing for this migration, to be scheduled for the first year of the contract, separately from the normal hosting costs (see Annex III Financial Offer form).

- Towards the end of the contract, the contractor will be required to provide ENISA recent backups of data and copies of the source code or binaries, together with a manual that explains how the website and portals can be set-up and operated in a new environment.

At the end of the contract the contractor is expected to facilitate the handover of the data and the source code and binaries to a new contractor or to a new environment, depending on the needs of ENISA. This could require parallel running of the website on the contractor's infrastructure and on another infrastructure

13. PLACE OF WORK AND DELIVERY

The implementation of the services will be undertaken at the contractor's premises.

One face-to-face kick off meeting between ENISA and the contractor might be held at ENISA's premises (either in Athens or Heraklion) depending on the restrictions imposed by the current ongoing COVID-19 pandemic. If a face-to-face meeting is not possible, the first and all other meetings between ENISA and the contractor can be made by using video conference systems, telephone or e-mail.

14. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

In this section it is outlined how ENISA expects the tenderer to structure its technical offer responding to this tender. In general, ENISA expects the tenderer to explain how the below mentioned requirements will be met by the tenderer.

14.1 WEB HOSTING

The tenderer shall provide a full description of the web hosting infrastructure, including technical details about how the detailed requirements are being met (physical security measures, physical redundancy, etc. - *please see sub-sections 2.1 until 2.8 above, as well as data protection requirements under Section 17 below.*

14.2 WEB DEVELOPMENT SERVICES

- Description of your company and how requirements in Section 4 are being met. 3 to 5 recent projects that show relevant expertise and experience in developing and maintaining similar websites or portals;
- 3 to 5 recent projects in developing similar Plone-based websites (if the above-mentioned projects do not involve Plone);
- The project team responsible for delivering the services, indicating the project manager and/or the technical experts that will be involved;
- CV's of members of the project team, clearly indicating their relevant experience in the Plone (and other platforms) web development field;
- Description of how you intend to deliver these services, addressing issues such as testing of new features, automated deployment in the test environment, automated deployment in the production environment, test data to test resolved bugs in the test environment and delivery of documentation;
- Quality control and assurance methodology;Data protection/privacy policy and/or any other relevant information with regard to compliance with Section 17 of this tender.
- Brief project plans, methodology to be used and estimation of man hours and budget, for fulfilling 4 change/development request scenarios as described below:

14.3 SCENARIOS - WEB DEVELOPMENT

The following four scenarios must be assessed and your estimations of volume of work required in 'person hours' per profile and overall project cost shall be entered into the appropriate boxes in the Financial Offer form (Annex III). These scenarios refer to a possible situation in accordance to ENISA needs, in order to facilitate the tenderer towards building a reliable and comparable financial offer. Hourly rates are also required to be provided in Part B of the Financial Offer form for the various requested profiles, which must then be used as the basis, together with estimation of person hours required,for each scenario. The actual projects to be awarded to the successful contractor will have a much more detailed level of technical specifications.

Failure to provide an estimation for each of the 4 scenarios may result in your offer being declared invalid and not further evaluated.

SCENARIO 1: UPDATE OF THE ENISA TOPICS SECTION

The topics section (https://www.enisa.europa.eu/topics) of the ENISA website is key to accessing ENISA's current work, deliverables, tools etc. Therefore it has to be improved so that access to information is facilitated. The following improvements must be taken into account:

- Mark the "Most Visited" topics
- Give the possibility to display topics alphabetically or ordered based on importance (importance to be manually specified by ENISA). The user should be able to select the preferred listing methodology and easily switch from one to the other.
- For each topic, display relevant linked content such as Publications, Topics, News, Events with links to the relevant pages.

SCENARIO 2: UPGRADE THE ENISA WEBSITE

Upgrade the ENISA website (https://www.enisa.europa.eu/) to the latest PLONE version.

SCENARIO 3: DEVELOPMENT OF A TRAINING INVENTORY

The ENISA website topic dedicated to Training for cybersecurity specialists (https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists), whose layout need to be improved. The section contains information like:

- Categories
- Short description
- Duration
- Handbook and manuals
- General information on courses

ENISA requirement is to develop a ''visual tool'' to display the training material in a more user-friendly way. In particular, the number of clicks needed to reach the final training should be reduced. An entry point page should be developed to quickly identify typologies of courses, a filter and a search bar should be included. The possibility to include ad hoc icons and pictures should be included (per course) as well as the possibility to add short explanatory videos and longer video training courses. The tool should be also easy to hand from a management point of view, as more courses will be added manually in the future.

The following elements should also be considered:

- Highlight key courses e.g. popular, covering trending topics, new etc. (selected by ENISA)
- Display all the areas for which courses are available in an easy, user friendly manner
- Listing of all courses on click or on hover
- Other elements can also be included e.g. number of downloads per course, date of the last update etc.

The transposition of current training material within the new layout is also required.

SCENARIO 4: DEVELOPMENT OF AN INTERACTIVE TOOL SUPPORTING STAKEHOLDERS

ENISA's requirement is to develop an online interactive repository of information and good practices as well as providing links to other ENISA work. The information should be displayed in a useful and customizable way. In particular, the tool should support input from a structured data set (e.g. csv, xlsx) and the end user should be able to customize every query (e.g. by using various parameters, filters drop, down menus etc.) in order to get the corresponding information.

The tool administrator should be able to add and customize the tool data as required (e.g. by adding new, editing or deleting one or more entries). It should also be possible to include links to other materials (internal and external).

It should also be possible to customize the tool adding the possibility to include visual materials. An example of a similar tool that can be used for reference is the following:

https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

15. CONTENT AND PRESENTATION OF THE FINANCIAL OFFER

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

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

16. TENDER RESULT AND ESTIMATED CONTRACT VALUE

The estimated overall maximum contract value without this being binding for ENISA is **nine hundred and fifty thousand Euros (€950,000.00)** over a maximum possible period of 4 years.

It is emphasized that a **maximum of one hundred and fifty thousand Euros (€150,000.00)** shall be assigned to 'Web Hosting services' over the maximum 4-year period - including the costs of the one-off 'Migration'

(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)).

17. DATA PROTECTION

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[2] ('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[3] (General Data Protection Regulation – 'the GDPR')** as concerns personal data processing carried out by the contractor on its proper behalf as a controller.

Processing of personal data by ENISA as contracting authority:

Information on the processing of personal data by ENISA as contracting authority in charge of the present procurement procedure is available in the Privacy Statement on the ENISA website as well as in Article II.9.1 of the draft contract in Annex IV. In this context, please be informed that ENISA may register your personal data as a tenderer or selected contractors in the Early Detection and Exclusion System (EDES) if you are in one of the situations mentioned in Article 136 of the Financial Regulation. The relevant Privacy Statement is available on the European Commission's website, here: http://ec.europa.eu/budget/explained/management/protecting/protect_en.cfm#BDCE.

Processing of personal data by the selected contractor:

Personal data processing in execution of the contract between ENISA and the selected contractors shall comply with Regulation (EU) 2018/1725 (the EDPR).

The processing of personal data shall happen in accordance with Article 29 of the EDPR. In particular, the selected contractor shall comply with the following:

- to process the personal data only on documented instructions of ENISA, in particular with regard to the purposes of the processing, the categories of data that may be processed, the recipients of the data and the means by which the data subject may exercise its rights;

[2] 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

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1–88

- to 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)[4], outlined in Art. 33 to 40 of the EDPR ;
- to make available to ENISA all information to demonstrate compliance with the obligations laid down in the EDPR and to allow for and to contribute to audits, including inspections, conducted by ENISA or another auditor mandated by ENISA;
- As concerns the localisation of and access to the personal data, to comply with the following:
    - the personal data shall only be processed and held in data centres within the territory of the European Union and the European Economic Area and will not leave that territory. This includes also any backup centres and location of backup data.;
    - the contractor may not change the location of data processing without the prior written authorisation of ENISA ;
    - The contractor shall inform ENISA in case of any need for transfer of personal data to third countries or international organisations and will perform such transfer only after written authorisation by ENISA. Any transfer of personal data to third countries or international organisations shall fully comply with the requirements laid down in Chapter V of the EDPR ;
    - The contractor shall notify ENISA without delay of any legally binding request for disclosure of the personal data processed on behalf of ENISA made by any national public authority, including an authority from a third country. The contractor may not give such access without the prior written authorisation of ENISA;
    - To contact the Data Protection Officer (DPO) of ENISA, in charge of monitoring data protection compliance, with any questions arising or in case of need for assistance concerning personal data protection dataprotection@enisa.europa.eu,

[4] http://www.edps.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.

18. OWNERSHIP, INTELLECTUAL, PROPERTY RIGHTS, USE OF RESULTS

As regards any product or delivery commissioned by ENISA and developed by the contractor in the context of the contract resulting from this call for tenders, as well as source codes of IT applications and models developed for ENISA, the intellectual property rights will be owned by ENISA only in its capacity as financial source of the contract. The contractor cannot file a trademark; patent, copyright or other IPR protection scheme in relation to any of the results or rights obtained by ENISA in performance of the contract, unless the contractor requests the ENISA ex-ante authorisation and obtains from ENISA a written consent in this regard.

ENISA does not acquire ownership or any license of pre-existing rights not incorporated in the deliverables. The full ownership is limited to the deliverables, which might include licensed pre-existing rights on excerpts, parts, texts etc., if fully or partially incorporated in the final deliverables.

The draft contract in Annex IV contains further provisions on ownership of intellectual property rights. All quotations or information the tenderer provides in the technical and financial offer for this tender, which originates from other sources to which third parties may claim rights, have to be clearly marked in the offer in a way allowing easy identification (source publications, including date & place, creator, number, full title etc.). The tenderer shall take account of the above specification on ownership and copyrights in their technical and financial offer.

19. 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.

20. 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.

21. PRICE REVISION

The price quoted must be fixed and not subject to revision during the first year of performance of the contract. From the beginning of the second year of performance of the contract, prices may be revised in accordance with Article I.3.3 of the framework contract

22. 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.

23. 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.

24. 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.

25. PAYMENT ARRANGEMENTS

Payments under the Contract shall be carried out within 30 days after an invoice is submitted to ENISA. Payments will be made after receipt and approval of the ordered services by ENISA. Each invoice must specify the specific services covered as per the relevant purchase order.

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.

For the ‘hosting services’ which will be ordered under a yearly Specific Contract, it is anticipated that an invoice will be issued by the contractor on a quarterly basis in arrears and in 4 equal instalments.

In other words, the first invoice, for a quarter of the total yearly amount for ‘hosting services’, will be due 3 months following the countersignature of the Specific Contract (under the Framework Service contract) by both parties.

While there is the possibility for negotiation on the abovementioned terms of payment, the Agency would prefer adherence to the stated terms.

26. 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 yearly 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 IV).

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

1. INFORMATION ON TENDERING

1.1 CONTRACTUAL CONDITIONS

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

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

Before the contract is signed, the Agency may decide to abandon the procurement procedure or cancel the award procedure without the tenderers being entitled to claim any compensation.

1.2 JOINT TENDERS (IF APPLICABLE)

A joint tender is a situation where a tender is submitted by a 'group' of economic operators (consortium). Joint tenders may include subcontractors in addition to the joint tenderers.

Tenders can be submitted by groupings of service providers/suppliers who will not be required to adopt a particular legal form prior to the contract being awarded. However, the Agency will require the grouping:

- Either to have the contract signed by all members (partners) of the grouping. In this case, one of them, as 'Lead Partner', will be responsible for the receipt and processing of payments for members of the grouping, for managing the service administration and for coordination of the contract;
- Or to have the contract signed by the 'Lead Partner' only, who has been duly authorised by the other members to bind each of them (a fully completed 'power of attorney' form for each member of the Group will be attached to the contract according to the template provided by the Agency).

In addition, the composition and constitution of the grouping, and the allocation of the scope of tasks amongst the members, shall not be altered without the prior written consent of the Agency, which can be withheld at its discretion.

In case of a joint offer, each member of the grouping shall provide the following:

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

- a **Declaration of honour with respect to the Exclusion Criteria and absence of conflict of interest** must be filled in, signed by (an) authorised representative(s), scanned and uploaded in the corresponding section.

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

1.3 LIABILITY OF MEMBERS OF A GROUP

Partners in a joint offer assume **joint and several liability** towards the Agency for the performance of the contract as a whole.

Statements, saying for instance:

- That one of the partners of the joint offer will be responsible[5] for only one part of the contract and another one for the rest, or
- That more than one contract should be signed if the joint offer is successful

are thus incompatible with the principle of joint and several liability. The Agency will disregard any such statement contained in a joint offer, and reserves the right to reject such offers without further evaluation, because they do not comply with the tendering specifications.

1.4 SUBCONTRACTING

Subcontracting is permitted in the tender but the contractor will retain full liability towards the Contracting Authority for performance of the contract as a whole.

If the tenderer intends to subcontract part of the service, they shall indicate in their offer which part will be subcontracted and to what extent (% of the total contract value).

Tenderers must ensure that Article II.7 of the contract (Annex IV) can be applied to subcontractors.

Tenderers must give an indication of the proportion of the contract that they intend to subcontract.

Tenderers are required to identify all subcontractors.

During contract execution, any change of a subcontractor identified in the tender will be subject to prior written approval of the Contracting Authority.

2. STRUCTURE AND CONTENT OF THE TENDER

2.1 GENERAL

Tenders must be written in **one of the official languages** of the European Union. The working language of ENISA is English.

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

Tenders must be written in a clear and concise manner, with continuous page numbering. Since tenderers will be judged on the content of their written bids, they must make it clear that they are able to meet the requirements of the specifications/terms of reference.

2.2 STRUCTURE OF THE TENDER

Based on the ***e-Submission*** environment[6], 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.

[6] *For detailed instructions on how to submit a tender please consult the e-Submission Quick Guide available at: https://webgate.ec.europa.eu/digit/opsys/esubmission/assets/documents/manual/quickGuide_en.pdf*

(ii) Financial identification

The tenderer (or the single point of contact in case of joint tender) must provide a Financial Identification Form and supporting documents. Only one form per offer should be submitted (no form is needed for subcontractors and other joint tenderers). The form is available at:

http://ec.europa.eu/budget/contracts_grants/info_contracts/financial_id/financial_id_en.cfm

Remark: Tenderers that are already registered in the Agency's accounting system (i.e. they have already been direct contractors **with ENISA** in the past) must provide the filled in form but are not obliged to provide the supporting evidence.

The form needs to be printed, filled in and then scanned and uploaded in the Qualification section. In case of a joint tender, it has to be uploaded in the ***"Documents"*** section of the Consortium Leader.

(iii) Power of Attorney

In case of a joint tender, an Agreement / Power of Attorney for each partner must be filled in, signed by (an) authorised representative(s), scanned and uploaded. Please choose 'Model A' for an ad hoc grouping or 'Model B' for a legally constituted consortium - see templates in Annex 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[7].

- 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)*

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

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

The completed Financial Offer form(s), MUST ALSO be uploaded in the relevant section:

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

3. ASSESSMENT AND AWARD OF THE CONTRACT

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

The aim of each of these stages is:

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

Only tenders meeting the requirements of each stage will pass on to the next evaluation stage.

3.1 EXCLUSION CRITERIA

Tenders will be rejected if they do not comply with applicable obligations under environmental, social and labour law established by Union law, national law and collective agreements, or by the international environmental, social and labour law provisions listed in Annex X to Directive 2014/24/EU and compliance with data protection obligations resulting from Regulation (EU) 2016/679 and Regulation (EU) 2018/1725".

All tenderers shall provide a 'declaration on their honour' (see Annex 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[8]. 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.

[8] 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

(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 **€350.000,00 (three hundred and fifty 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 of 350.000,00 EUR.

(c) If tenderers will call on the competences of another entity (for example, a parent company), a written undertaking by the said entity certifying that it will make available to the tenderers the resources required to implement the contract.

If for some exceptional reason which the Contracting Authority considers justified, the tenderer is unable to provide the documentary evidence requested above, he may prove his economic and financial capacity by any other means which the Contracting Authority considers appropriate, but only following a formal request for clarification **<u>before</u>** the tender expiry date.

3.2.3 TECHNICAL AND PROFESSIONAL CAPACITY CRITERIA AND EVIDENCE

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

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

- Details of the structure of the organisation
- A detailed description of the resources (hardware & software) to be made available for this contract, subject to the contractual clause on subcontracting;
- Provide a statement confirming that the tenderer fulfils the general requirements of Regulation (EU) 2016/679 ('the GDPR') and that in particular it will comply with the specific requirements of Regulation (EU) 2018/1725 (the EDPR) in its service provision to ENISA with reference to the obligations on personal data protection listed in Part 2 - Section 17 of these tender specifications;"
- Curriculum Vitae (CV) of the management staff and other staff related to the provision of services requested - providing as a MINIMUM the following profiles (*please note that the actual quality and relevance of the CVs for each profile will be assessed in the Award Criteria section below*);
    - **Project Manager** (2 CVs)
    - **Business Analyst** (1 CV)
    - **Developer** (5 CVs)
    - **Graphical Interface Designer** (2 CVs)
    - **Quality Assurance/ Tester/ DevOps** (2 CVs)
- Quality control and assurance methodology;

- List of the main hosting services performed in the past 3 years, with details of the values, dates and public or private recipients enclosing, where possible, documents concerning reliability and efficiency of the services performed issued by the beneficiaries of the service;
- List of the main web development services performed in the past 3 years based on the Plone platform as well as other platforms, with details of the values, dates and public or private recipients. Where possible, provide evidential documents concerning reliability and efficiency of the services performed - issued by the beneficiaries of the service.

3.3 COMPLIANCE WITH TENDER SPECIFICATION AND MINIMUM REQUIREMENTS

Your offer will be assessed for compliance with the tender specifications prior to its assessment against the award criteria.

Tenders do not comply with the tender specifications and will be rejected if they:

- do not comply with minimum requirements laid down in the tender specifications;
- propose an alternative solution from the one imposed;
- propose a price above the fixed maximum set in the specifications;
- are submitted as variants, when the specifications do not authorise them;
- do not comply with applicable obligations under environmental, social and labour law established by Union law, national law and collective agreements or by the international environmental, social and labour law provisions listed in Annex X to Directive 2014/24/EU9 and compliance with data protection obligations resulting from Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.

These grounds for rejection are assessed before the award criteria stage, so in the case of non-compliance, this tender will not be evaluated. The tenderer will thus be informed of the grounds for rejection without being entitled to receive feedback on aspects of the tender other than on the non-compliant elements.

3.4 AWARD CRITERIA

3.4.1 QUALITY OF THE OFFER

Once the Tenderer has demonstrated the appropriate capacity to perform the Contract on the grounds of the selection criteria, the offer will be assessed based on the award criteria.

No	Qualitative award criteria		Weighting (max. points)
1.	**Technical compliance**	Compliance with the technical requirements (Part 2 of this document) as well as information on compliance with EDPR requirements under Part 2 - Section 17 of the tender.	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 scenario solutions offered.	30
3.	**Project Team**	Experience, expertise and relevance of the proposed team proposed for delivering the required services and to manage ENISA's projects.	30
Total Qualitative Points (QP)			**100**

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

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 quality 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 technical specifications. 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.

3.4.2 PRICE OF THE OFFER

Tenderers must provide prices (in Euro) in **each** blank box as shown in Annex III – 'Financial Offer form' – failure to provide a price in each box may lead to exclusion of your offer.

The total bid price ratio '$\mathbf{P_B}$' will be calculated using the following formula and weightings:

$$\mathbf{P_B = [(P_H / P_{HC}) \times 20] + [(P_{SC} / P_{ST}) \times 40] + [(P_{DC} / P_D) \times 40)]}$$

where:

P_H = Hosting cost

P_D = Web Development consolidated cost (P_1 +P_2 + P_3 + P_4 + P_5 + P_6)

P_{DC} = Cheapest P_D

P_{ST} = Total Scenario cost (S_1 + S_2 + S_3 + S_4)

P_{SC} = Cheapest P_{ST}

P_{HC} = Cheapest P_H

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

3.4.3 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:

$$\mathbf{TWP = (Q_P \times 0.7) + (P_P \times 0.3)}$$

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 **23rd June 2020 at 11:30 EEST Eastern European Summer Time (Greek local time)** at ENISA Athens office, 1 Vasilissis Sofias Street, Maroussi 151 24 Attiki, Greece.

A maximum of one legal representative per participating tenderer may attend the opening session. Tenderers shall inform the Agency in writing of their intention to attend, by email to procurement@enisa.europa.eu **at least 2 working days** prior to the opening session.

Alternatively, please note *that all tenderers may simply request a copy of the Opening Report to be sent to them by email after the conclusion of the Opening Session procedure.*

5. OTHER CONDITIONS

5.1 VALIDITY

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

5.2 LOTS

This Tender is not divided into Lots.

5.3 ADDITIONAL PROVISIONS

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

5.4 NO OBLIGATION TO AWARD THE CONTRACT

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

6. SPECIFIC INFORMATION

6.1 TIMETABLE

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

Title: "**Web Hosting and (Plone) Web Development services"**

ENISA F-COD-20-T18

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	18th May 2020	
Deadline for request of information to ENISA	15th June 2020	
Last date on which clarifications are issued by ENISA	16th June 2020	
Deadline for **electronic reception** of offers via ***e-Submission***	**22nd June 2020**	**18:00 CEST** Central European Summer time
Opening of offers	23rd June 2020	**11:30 EEST** Eastern European Summer **(Greek local)** Time
Date for evaluation of offers	TBA	TBA
Notification of award to the selected candidate + 10 day standstill period commences	TBA	Estimated
Contract signature	TBA	Estimated