ANNEX I.B

IT infrastructure hosting services for the Agency for the Cooperation of Energy Regulators

Framework Contract

CASE STUDY

OPEN CALL FOR TENDERS

ACER/OP/MMD/12/2013

Table of Contents

1. Introduction

The tenderer shall submit a detailed proposal in writing on the basis of the case study presented below, which provides for hosting services for the Agency for a period of one (1) year.

The case study is a fictional exercise and does not commit the Agency to place such a request for service, should the tenderer be awarded the Framework Contract.

2. The content of the case study

The tenderer's proposal for the case study shall include at least the following documents/information and the proposal should be limited to maximum 50 pages A4:

a) a brief description of the approach the tenderer intends to adopt during the implementation of the case study;
b) a detailed description of the hardware proposed (type, model, brand, quantity, features, software provided, if possible provide a brochure for each component);
c) usage matrix containing each platform component and the role in the entire platform (e.g. Server X – Database Server);
d) a detailed list of tasks to be completed by the proposed experts, and the usage of each single expert profile using the list of expert profiles as described by the Agency in the technical specifications. If a profile is missing in the Agency's list, the tenderer should add the proposed profile following the template of the Agency;
e) a detailed time schedule (i.e. GANTT chart) listing the tasks from the point above on a time line as well as the use of human resources per profile in terms of man days;
f) a detailed proposal of Network Topology;
g) a detailed proposal for security to be applied to the case study;
h) a detailed proposal of the Service Level Agreement for the entire duration of the case study;
i) a detailed financial proposal applicable to this case study. The financial proposal shall be based on the tenderer's financial offer and/or the tenderer's detailed official price list.

IMPORTANT: The tenderer shall indicate where in the tenderer's financial offer and/or in the detailed official price list each proposed service/activity/etc. is specified. This financial proposal shall be used as a total all inclusive price for the evaluation of the tenders as specified in Annex I tender specifications.

The financial proposal may include out of price list products, nevertheless this need to be described and justified as defined in point 9.2 "Ordering procedure" in Annex I Tender Specifications.

3. Description of the case study

The Agency intends to launch a service request with the aim to cover the need to establish a working hosted system to host a Market Monitoring software platform which should serve 28 NRAs and the Agency.

The Agency proprietary software will be based on a 3 tiers application with the following components:
- a Web Server – used to serve the Web Interface or to expose Web Services;
- an Application Server – used to process the Business Logic;
- a DB Server – used to store and retrieve data in a fast way.

The system should also be able to host the following ancillary services which are essential for the proper work of the Agency's proprietary software:

- SMTP service;
- an authentication service;
- a Terminal Server (RDP based);
- several computational nodes which must be able to process in near real time around 2 Terabytes of data;
- DNS, DHCP and any basic networking service to interconnect the proposed systems.

3.1. Software used by the Agency in the existing test environment

- Operating System: Microsoft Windows 2008 R2, Red Hat Linux 6.1 on hardware and/or on virtualised environment VMWARE vSphere 5.
- Application Server: JBoss and Liferay.
- Data base: Oracle 11g R2.
- A custom made set of Energy Market Monitoring applications which are able to run parallel jobs on several Servers using a shared storage and coordinating on a TCP/IP standard Local Area Network.
- A federated authentication server which must be able to easily manage a community of 30.000 users with the interconnection of 29 repositories and centralised authorisation engine.

3.2. Sizing

The Agency estimates that in one year it will store on average 2.000 GBytes of data inside its databases, and will need to run daily jobs on the entire amount of data in order to analyse them and identify possible threats to the Energy Markets.

The Agency has estimated that it may need the following building blocks in order to achieve the goal to have a working system at the primary site, but will need also to be provided with a Disaster and Recovery site in a secondary location which must be placed in the same service request:

- A: Cage on primary site;
- C: 2 Racks;
- D1.2: 3 Standalone servers;
- D2.2: 8 Blade;
- D3: 1 Storage Area Network unit;
- D4: 2 Network connectivity devices – switches;
- D4: 2 Network connectivity devices – core switches;
- D5: 4 Network security devices;
- D6: 1 Backup device;
- F1: 27.6 TB of net storage capacity;
- F2: 50 TB backup capacity;
- G5: 2 x 100 Mbps connection to the internet (1 for primary and 1 for secondary site);
- G1: 1 x 10 Mbps connection between primary site and Agency's premises;
- H1.1: Hypervisor for 32 physical CPUs in blade servers;
- H2.2: 12 Windows 2008 R2 Datacentre + 72 RHEL 6 operating systems (6 + 36 on primary and 6 + 36 on secondary site);
- H3: 42 Backup Software (for OS instances on primary site);
- H4: 2 instances of BC/DR Software Solution (for replicating data between primary and secondary site);

- H5: 12 instances Anti-malware Software (for Windows OS);
- H6: 2 instances of Monitoring and Surveillance Software (for primary and secondary site);
- J1: 24x7 Service Desk Support for the provided services for 200 incidents per year;
- J2: Monitoring, Surveillance and Reporting/Alerting for all listed equipment;
- J3: System Administration for all the requested services for one year;
- J4: 50 man days WOC (working outside the country) for Custom Support Services;
- J4: 50 man days WIC (working inside the country) for Custom Support Services;
- J5: 25 man days WIC (working inside the country) for Project Management Services (A-level profile as per Annex I.A technical specifications);
- J5: 25 man days WOC (working outside the country) for Project Management Services (A-level profile as per Annex I.A technical specifications);
- 25 man days WIC (working inside the country) for B-level profile as per Annex I.A technical specifications;
- 25 man days WOC (working outside the country) for B-level profile as per Annex I.A technical specifications;
- 25 man days WIC (working inside the country) for C-level profile as per Annex I.A technical specifications;
- 25 man days WOC (working outside the country) for C-level profile as per Annex I.A technical specifications;
- K1: 16 public IP addresses;
- K2: 3 domain names (.eu);
- K3: 16 DNS entries.

3.3. Availability constraints

3.3.1. The proposed platform should fulfil the following requirements:

- Each component must offer high availability of internal components (e.g. a minimum of two separate power units).
- For the Web Servers an active-active configuration needs to be provided.
- For Application Server an active-active configuration needs to be provided.
- For Oracle server an active-passive configuration needs to be provided.
- Backup needs be provided and must assure recovery of the working system within 24 hours after destruction of the primary site and in case the secondary date is not available.

3.4. Security

The Case Study shall detail out the tenderer's proposal for a security infrastructure which must be reflected in the financial proposal for the case study. The proposed security infrastructure must contain security devices including firewalls, proxies, Intrusion Detection Systems, Anti Virus, etc.

3.5. Connectivity constraints

Connectivity must be assured to the system end-users with an internet secure communication channel. The Agency will provide SSL certificates for the web server. All the other layers of the hardware platform should be secured as much as possible and in a transparent way. Peaks of 2.000 concurrent sessions may take place especially during the launch phase of the system. The Agency's software is able to support such peaks. All

components provided in the case study (hardware and each piece of equipment) must be able to assure the same level of performance.

The system will need to provide each of the 28 NRAs and the Agency with a secure communication channel in order to process all the requests forwarded from/to the Agency and from/to the NRAs. Easy and manageable solutions based on VPN appliances are the preferred Agency's option. In order to reduce costs, the Agency will rely on existing internet connectivity at the NRAs side, and will allow the adoption of a central appliance at the hosting site. This need needs to be reflected in the proposed infrastructure.

A secure connection channel with the hosting provider shall be provided to the Agency. The secure connection channel shall be able to reach the hosted hardware and to provide any operation, including remote hardware reset of each provided component. A dedicated connection is the Agency's preferred option. In this respect, as security devices can assure a reasonable level of security, the Agency encourages the use of low cost solutions, i.e. VPNs with the use of dedicated xDSL lines. The Agency will not rely on the existing lines as they are already used for other purposes (web site and others). The proposal for the case study shall include a communication line together with all the equipment to secure it.

4. Services to be provided by the tenderer

- Installation of a fully working platform fully implementing the topology and the hardware configuration.
- Installation of Operating Systems.
- Installation of Data Base Systems.
- Installation of Application Servers.
- Installation of all listed ancillary services.
- All security configurations as proposed.
- Configuration and basic test connectivity of DB vs Application Server, Web Server vs Application Server, proposed security platform vs Web Server.
- Configuration of each connectivity channel.

5. Services provided by the Agency or by a third party

- Installation of the Agency's proprietary software and its configuration.
- Configuration of high availability platforms for the Agency's proprietary software.