ANNEX II + III : TECHNICAL SPECIFICATIONS + TECHNICAL OFFER

Contract title: Supply of equipment necessary for establishing the secondary/backup Treasury Data Centre **p 1 /…**

Publication reference: EuropeAid/137122/IH/SUP/RS

Column 1-2 should be completed by the Contracting Authority
Column 3-4 should be completed by the tenderer
Column 5 is reserved for the evaluation committee

Annex III - the Contractor's technical offer

The tenderers are requested to complete the template on the next pages:

- Column 2 is completed by the Contracting Authority shows the required specifications (not to be modified by the tenderer),
- Column 3 is to be filled in by the tenderer and must detail what is offered (for example the words “compliant” or “yes” are not sufficient)
- Column 4 allows the tenderer to make comments on its proposed supply and to make eventual references to the documentation

The eventual documentation supplied should clearly indicate (highlight, mark) the models offered and the options included, if any, so that the evaluators can see the exact configuration. Offers that do not permit to identify precisely the models and the specifications may be rejected by the evaluation committee.

The offer must be clear enough to allow the evaluators to make an easy comparison between the requested specifications and the offered specifications.

Unless otherwise specified, the requirements in these Technical Specifications are presented as a minimum standard which the offered goods must meet.

Introduction

Primary Data Center of the Treasury Administration is situated in Belgrade (7-9 Pop Lukina street), and secondary site is located in Novi Sad (Modene 7).

EMC VNX8000 Unified Storage as the primary storage system is currently used on primary Data Center. The data replication between the two sites is carried out through the EMC RecoverPoint devices. The creating and storing of the backup data copies is carried out via the special purpose backup devices, EMC DataDomain 2500 on primary and DataDomain 670 on secondary site.

Servers for FMIS (BEX component) are Unix Fujitsu (Oracle) cluster on primary and one server on secondary site. Other services are running on VMware (blade servers) on both sites.

Network infrastructure is based on Cisco solutions, redundant core, SAN and WAN switches.

Security system is based on IBM IPS and firewall devices.

Implementation requirements

General

Item Number 1

The Contractor will be responsible for the successful implementation of Storage system.
The implementation includes:

- Installation, setup and configuration of the equipment,
- Connecting to an existing network and power infrastructure.
- Setting up replication between the primary location and secondary site of the Treasury.

Item Number 2

The Contractor will be responsible for the successful implementation of Devices for network balancing.
Installation and configuration of the equipment includes:

- Installation and configuration of the equipment at the secondary site
- Connecting devices to existing network equipment and systems for uninterrupted power supply. It is necessary to provide cables and modules.
- Testing and commissioning.

Item Number 3

The Contractor will be responsible for the successful implementation and commissioning of IPS solution.
IPS system implementation services include the following activities: installation, configuration, and integration into the existing IT environment of Beneficiary and commissioning, with the minimum possible impact on the operation of existing services. Contractor is expected to do the security assesment, planning and project management, equipment installation, customization of IPS solution to client's needs, test plan, test and verification of the implementation of the solution, preparation of project documentation and built documentation and training of the IT staff of Beneficiary.
Implementation of IPS system is carried out by the Contractor and the Beneficiary.

The Beneficiary shall provide all relevant documentation and technical assistance related to the existing environment, as well as the participation of professional IT staff responsible for the operation of specific services.

Address of the primary site of the Treasury is: Pop Lukina 7-9, 11000 Belgrade.

Address of the secondary site of the Treasury is: Modena 7, 21000 Novi Sad.

Delivery list

All equipment is to be delivered to the secondary site of the Treasury, Modena 7, 21000 Novi Sad.

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
1	**Storage**			
1.1	Storage system must meet the relevant requirements and be functional as a single unit (storage virtualization, or building solution from more different physical components is not allowed).			
1.2	The system must be rack mount type, modular, scalable, suitable for additional upgrade. Rack and all necessary accessories for the assembly to rack mount must be included.			
1.3	All active hardware components must be redundant („no single point of failure") and interchangeable, without interruptions in operation (hot swap components). Cache memory must be battery backed up and there must be a mechanism for saving data from cache memory to disks in case of the entire break in the supply.			
1.4	Storage system must be Unified system • Storage system must have SAN connectivity (FC and FCoE) on the system itself • Storage system must have NAS connectivity (CIFS and NFS) on the system itself or via gateway device. File access (NAS) may also be implemented via specialised gateway devices, whereas, in such case, all mentioned requirements are related to the system itself without gateway devices. Gateway devices must be offered with redundant controllers (at least 2 of them) operating in active – active mode of operation. It is deemed that gateway device only enables access to CIFS and NFS protocols and its technical characteristics are not			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
	considered as characteristics of storage system. If file access is implemented via gateway device, it is not necessary that the offered storage system and gateway devices are from the same manufacturer.			
1.5	The system must support the following RAID levels: 1, 5 and 6 or the equivalent functional implementations.			
1.6	The system must be fully accessible under the conditions of use of all new versions of software Microsoft operating systems, as well as in case of mostly used Linux operating systems, Solaris, HP-UX and VMware.			
	Hardware properties of the storage system			
1.7	Storage system must have at least 1TB usable Read and Write cash memory in total intended for SAN access.			
1.8	Cache memory must be controller based memory or made by adding specialized SSD drives that presents as Read and Write cache memory to controller units, and may not be implemented by adding external caching devices.			
1.9	Communication subsystem consists of combinations of FC, FCoE and Ethernet ports. It is necessary that the system contains at least following configuration in total: o 8 ports 8Gbps FC for block access o 4 ports10Gbps Native FCoE for block access (TWINAX Copper) o 8 ports 10GbE TWINAX Copper ports for file access (CIFS/NFS) o It is necessary to provide cables and modules.			
1.10	Storage system must be scalable up to minimum 500 drives without virtualised connections of several devices.			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
1.11	Storage system must support 2.5" and 3.5" disk drives in the same system.			
1.12	Memory (SSD/Flash) discs. The installed discs must have minimum 4 TB of nominally declared gross capacity. Bidder must offer at least 20 physical drives. This capacity implies drives used only for data, and it does not include possible drives used as cache drives, if such a technology is offered. All offered drives from this category must be the same. Additionally, system must have hot spare drives of the mentioned type.			
1.13	SAS discs. The installed drives with SAS 6Gbps must have minimum 84 TB of nominally declared gross capacity. All offered drives from this category must be the same, and the spinning velocity not less than 15.000 rpm. Additionally, system must have hot spare drives of the mentioned type.			
1.14	NL SAS discs. The installed NL SAS drives of high capacity must have minimum 204 TB of nominally declared gross capacity. All offered drives from this category must be the same, bidder must offer minimum 102 physical drives, and the spinning velocity not less than 7,200 rpm. Additionally, system must have hot spare drives of the mentioned type.			
	Software functions of the storage system			
1.15	It is required that system configuration, supervision and management is based on the access via web-presentation system.			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
1.16	It is required that system has software for automatic tiering at sub-LUN level between different types of drives, without influence on availability of data, in order to achieve optimum performances. Tiering software must support data movement within pool of drives, pool can consists of all 3 kinds of drives (SSD, SAS and NL-SAS). It is necessary to offer this software for the entire offered capacity of storage system.			
1.17	It is required that system has software for virtualisation and utilisation of physical capacity (Thin/Virtual provisioning), for the entire offered capacity of storage system.			
1.18	It is required that system has software for migration of data from the existing system to a new one. The licence for this software must cover the entire offered capacity of storage system.			
1.19	It is required that system has software for creation of instant and full volume copies of the production (Snap and Clone) at file and block levels, for the entire offered capacity of storage system.			
1.20	It is required that system has software for supervision and monitoring and historic data reporting capabilities. Possibility to create custom reports of performances and capacities of storage system for the entire offered capacity of storage system.			
1.21	It is required to include block based deduplication or compression for the whole offered capacity, including SSDs and mechanical disks.			
	Solution for replication, functions and features			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
1.22	Solution for replication cannot be based on the technology of external storage virtualization. It can be based on existing EMC RecoverPoint GEN5 platform or equivalent.			
1.23	Data replication must support simultaneous synchronous and asynchronous remote replication with existing storage EMC VNX8000.			
1.24	Data replication must enable simultaneous synchronous and asynchronous local and remote replication, automatic switching from synchronous to asynchronous and vice versa, making local and remote copies, either according to the principle of manual make or according to time schedule defined in advance – according to the principle of whole copies, incremental changes and breakdown of conditions.			
1.25	The software and the solution for replication must integrate and enable non disrupted synchronous and asynchronous replication to the existing EMC VNX 8000 storage system. Additionally, Solution for replication, beside block based requirements, has to include license for replication on file (NAS) level with existing VNX8000 Unified storage system. Bidder can leverage existing replication technology that customer already has or offer its own replication solution that meet all requirements.			
1.26	The software used for data replication between locations must cover the total RAW offered capacity of storage system and not less than 270 terabytes.			
1.27	Solution for replication must have deduplication and compression functionality in order to save the link resources between locations.			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
	Implementation			
1.28	The Contractor shall deliver all equipment within a period not longer than 45 calendar days from the commencement date.			
1.29	The maximum period of time for implementation of the proposed solution system is 75 calendar days.			
	Warranty services			
1.30	One year warranty after provisional acceptance in accordance with the conditions laid down in Article 32 of the General Conditions, including technical support services. Response time: maximum 30 minutes for response by mail and/or phone against incident report and/or technical support submitted by the beneficiary Solution time: maximum 24 hours from the incident report and/or technical support. • Technical support during the warranty period includes:			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
	○ Collection, analyses and diagnostics of incident reports and execution of remedial actions ○ Installing software (including operating system) patches and updates ○ Constructing and regular updates of the system knowledge data base and technical documentation ○ Ensuring safe on-line access of the beneficiary to the system knowledge data base and technical documentation			
1.31	Technical support during the warranty period Provide 20 working days of engineering support, during the warranty period offered. These days can be used for system engineering support, consultation, counseling, transfer of knowledge in the areas of administration, installation, use and maintenance of the equipment offered for the duration of the maintenance contract.			
2	**Devices for network balancing (Quantity 4)**			
2.1	The system must provide at least 16x 10GE SFP+ interfaces			
2.2	Each device must have port for out of band management			
2.3	Each device must have redundant AC power supply			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
	Device performance (per device)			
2.4	Minimum L7 flow 20 Gb/s expandable with licensing unlock to 100 Gb/s (without adding additional hardware appliance / blade)			
2.5	System must include at least 5 and support for up to 25 independent virtual instances with full isolation of resources (CPU, Memory, SSL)			
2.6	The system must support at least 22.000 new SSL TPS (2048-bit Keys)			
2.7	Integrated and fully licensed Web Application Firewall / PCI-DSS v.3.0 compliant			
2.8	Web Application Firewall Throughput must support 13 Gb/s in Basic Mode (positive model) and be upgradeable to 29 Gbps			
	Application monitoring – each device must support:			
2.9	Monitoring and discovering applications using ICMP, TCP and UDP protocols			
2.10	Monitoring the validity of the work of HTTP and HTTPS applications on the Web page from a specified content			
2.11	Monitoring and discovering applications using LDAP, LDAPS, FTP, SNMP, DNS, NNTP, POP3, RTSP, RADIUS Authentication, SSL Hello and SIP UDP/ SIP TCP protocols			
2.12	Monitoring physical port functionality			
2.13	Monitoring the validity of the work based on Layer 2 (ARP), Layer 3 (PING), Layer 4 (TPC / UDP port check).			
2.14	Monitoring the validity of the work based on pre-defined Layer 7 inspection (HTTP, HTTPS, LDAP, SMTP, etc...), as well as specially customized Layer 7 inspection for any			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
	binary or text-based protocol.			
2.15	Advanced monitoring of proper operation of an application with the ability to determine the status of the server, based on the analysis of data obtained by checking the validity of the work.			
2.16	Setting time interval for monitoring			
2.17	Trending and reporting for web application performance service level management			
2.18	Setting the minimum number of attempts for each monitor before a real server is declared unavailable.			
2.19	Multiple validation control using IP address and port			
	Network traffic redirection			
2.20	Load balancing for layers 4-7 (OSI) reference model with support for IP, TCP and UDP protocols			
2.21	Load balancing for layers 4-7 on the Source and destination IP addresses			
2.22	Load balancing for layers 4-7 based on the application content (URL, cookie, header field, text, HTML tag, XML tag, DNS domain, query type).			
2.23	Load balancing based on response speed applications, the incoming and outgoing bandwidth, number of concurrent users, the relative weight of user-defined SNMP (MIB) data, the minimum number of connections, static or dynamic cookie			
2.24	Balancing based on cyclic (round-robin) and hash traffic			
2.25	Support for at least 1024 Virtual IP (VIP) address			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
2.26	White and black lists for redirecting traffic			
2.27	The virtual server is listening UDP and TCP port or range of ports			
2.28	Redirect the request to the next server group based on Layer 7 content, user-defined groups of destination server ports			
2.29	Activation and deactivation of the server behind the virtual address			
2.30	Policy-based bidirectional rewriting of HTTP header and payload elements			
2.31	Policy-based URL rewrite			
2.32	Custom responses and redirects & Policy-based routing			
	Session sustainability			
2.33	Session sustainability based on Layer 3 and 4 protocols			
2.34	Session sustainability based on the source IP address, cookies, SSL session ID, IP hash and values of HTTP headers			
	Adjustments and modifications			
2.35	Cookie insertion of sustainability sessions			
2.36	Adding, modifying and deleting data in the HTTP/S request and response headers			
2.37	Importing the client source address in the Layer 7 header			
2.38	Changing the URLs in the HTTP request and response packet			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
2.39	Bidirectional automatic update of URLs in the HTTP package			
2.40	Modify the HTTP content, to hide the identity and structure of the server			
2.41	Scripts for HTTP and other traffic			
	Global Server Load Balancing			
2.42	Load balancing over geographically remote locations			
2.43	The recovery in the event of link failure between data centers in active-active or active-backup mode			
2.44	Global redirecting of traffic based on DNS			
2.45	Resolve A and AAAA record DNS and DNSSEC queries			
2.46	Support of DNSSEC for securing the DNS infrastructure			
	Redundancy			
2.47	VRRP protocol, active-active, active-backup configuration			
2.48	Transfer of the active session to the backup device (stateful failover)			
2.49	Different instances of the device can establish a high availability with a variety of hardware devices			
	Layer 2 features			
2.50	802.1Q standard			
2.51	LACP (802.3ad) and static link aggregation			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
2.52	Support for Virtual eXtensible Local Area Networks (VXLANs)			
	Layer 3 features			
2.53	IPv6			
2.54	RIP-I, RIP-II, OSPF			
2.55	NAT			
2.56	Support for OSPF, RIP1/2, BGP			
2.57	Support for routing or transparent mode			
	Application acceleration			
2.58	SSL offload			
2.59	Import and export SSL certificates in PEM and PKCS # 12 format			
2.60	TCP multiplexing			
2.61	HTTP compression			
2.62	Web caching in accordance with RFC 2616 for HTTP 1.1, or the option to change behavior according to RFC			
2.63	Caching for static and dynamic application content			
	Traffic shaping and QoS			
2.64	Multiplexing, Buffering, Connection Keep-alive			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
2.65	Windows Scaling, Selective Acknowledgement, Fast Ramp			
2.66	TCP Westwood support			
	Data protection			
2.67	DoS, DDoS, SynFlood protection			
2.68	Filter traffic based on Layer 3, Layer 4 and Layer 7 information			
2.69	Control and management of traffic and bandwidth			
	Monitoring and reporting			
2.70	Generating logs and sending an alarm in the event of reduced device performance via email, SMS and SNMP protocol			
2.71	Manual or automatic report generation			
	Device administration			
2.72	Manage the device via the console cable through the CLI			
	Implementation			
2.73	The Contractor shall deliver all equipment within a period not longer than 45 calendar days from the commencement date.			
2.74	The maximum period of time for implementation of the proposed solution system is 75 calendar days.			
	Warranty services			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
2.75	Contractor is required to comply with the guaranteed service type, service 11x6x6. Under 11x6x6 service means a service availability of support from the developer within 11 hours from 7:30 to 18:30, 6 days a week (Monday to Saturday), the response after receiving request in a period not longer than 30 minutes, recovery (returning network equipment in functional state) not longer than 6 hours and solution time not longer than 4 weeks. • Technical support during the warranty period includes: o Collection, analyses and diagnostics of incident reports and execution of remedial actions o Installing software (including operating system) patches and updates o Constructing and regular updates of the system knowledge data base and technical documentation o Ensuring safe on-line access of the beneficiary to the system knowledge data base and technical documentation			
2.76	Under the technical support of the equipment, Contractor is obliged to: - Provide 30 working days of engineering support, during the warranty period offered. These days can be used for system engineering support, consultation, counseling, transfer of knowledge in the areas of administration, installation, use and maintenance of the equipment offered for the			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
	duratin of the maintenance contract.			
3	**Network Intrusion Prevention System**			
	Hardware features			
3.1	The system must be in the form of physical devices (appliances). Physical devices and software solution installed on them must be from the same manufacturer.			
3.2	The system must include primary and Failover device in High Availability configuration			
3.3	The system must have 8 x 1GbE Tx, 2 × 10GbE SR and 4 x 1GbE SX interfaces all with built in bypasses. It is necessary to provide cables and modules.			
3.4	The system must have redundant power supplies and redundant storage			
	Software features			
3.5	The system must support 10 Gbps of real inspected traffic and at least 220.000 connections per second			
3.6	The system must support 10 million simultaneous sessions (concurrent sessions) and the maximum delay of less than 150 micro seconds			
3.7	The system must allow inspection of at least 400 different protocols			
3.8	The system must provide (without additional devices and software) web application protection, application control, IP Reputation and SSL traffic inspection.			
	Implementation			
3.9	The Contractor shall deliver all equipment within a period not longer than 45 calendar days from the commencement			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
	date.			
3.10	The maximum period of time for implementation of the proposed solution system is 75 calendar days.			
	Warranty services			
3.11	One year warranty after provisional acceptance in accordance with the conditions laid down in Article 32 of the General Conditions, including technical support services. Response time: maximum 30 minutes for response by mail and/or phone against incident report and/or technical support submitted by the beneficiary. Recovery time in operating condition within no more than 6 hours from the incident report and/or technical support. Solution time: maximum 24 hours from the incident report and/or technical support. • Technical support during the warranty period includes: o Collection, analyses and diagnostics of incident reports and execution of remedial actions o Installing software (including operating system) patches and updates o Constructing and regular updates of the system knowledge data base and technical			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
	documentation o Ensuring safe on-line access of the beneficiary to the system knowledge data base and technical documentation			
3.12	Under the warranty maintenance of equipment, Contractor is obliged to: - Provide 30 working days of engineering support, during the warranty period offered. These days can be used for system engineering support, consultation, counseling, transfer of knowledge in the areas of administration, installation, use and maintenance of the equipment offered for the duration of the maintenance contract. - To carry out the inspection of the delivered equipment			
4	**Certified training**			
4.1	• **Certified training for Storage Administration** for minimum two employees (minimum duration – 5 working days). Training where participants will get certificate issued by the manufacturer of the equipment.			
4.2	• **Certified training for RecoverPoint Management** for minimum two employees (minimum duration – 3 working days). Training where participants will get certificate issued by the manufacturer of the equipment.			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
4.3	• **Certified training for Devices for network balancing - Essentials and Networking** for minimum four employees (minimum duration – 5 working days). Training where participants will get certificate issued by the manufacturer of the equipment.			
4.4	• **Certified training for Devices for network balancing – Implementing for App and Desktop Solutions** for minimum two employees (minimum duration – 5 working days). Training where participants will get certificate issued by the manufacturer of the equipment.			
4.5	• **Certified training for Network Intrusion Prevention System Administration** for minimum four employees (minimum duration – 5 working days). Training where participants will get certificate issued by the manufacturer of the equipment.			
4.6	• **Certified training for ISO 27001 – Information Security Management Systems** for minimum two employees (minimum duration – 5 working days).			
4.7	• **Certified training COBIT 5 Foundation** for minimum two employees (minimum duration – 3 working days).			
4.8	• **Certified training for Business Continuity Management** for minimum five employees (minimum duration – 4 working days).			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
4.9	The maximum period of time for implementation is 180 calendar days.			