Request for Proposal

Firewalls and Switches

Maldives Pension Administration Office (MPAO) is accepting bids for supply, installation and configuration of firewalls and network switches at MPAO.

SECTION I

1.0 Submission Requirements

1.1 All Proposers are required to express interest by sending an email to admin@pension.gov.mv

1.2 The complete original proposal must be submitted in a sealed package. Proposal shall be marked **Firewalls and Network Switches**. Proposer shall file all documents necessary to support their proposal and include them with their proposal.

1.3 Executive Summary: A summary of the Proposer's document and approach to the installation of systems of this kind and identify any unique or distinctive features of the system of particular interest to the evaluators based on the needs specified in this document.

1.4 Proposer and/or Partner(s) overview and background: The Proposer must provide basic information on the Proposer and any partners or subcontractors participating in the tender. This information should include, but not limited to, the history of the organization, its experience and its experience in the IT field, technical capabilities, experience implementing similar architecture, the size of implementations and success stories. This section should also explain any partnering arrangements that have been made to respond to the proposal.

1.5 Proposal Format: Proposal shall be submitted in the following format and include the following information.

1.5.1 Detailed description of Firewalls and Switches.

1.5.2 Detailed Cost for each item and services.

1.5.3 The Proposer should provide a reference of successful implementation of similar system and should include descriptions of system implementations they have completed. The mentioned project references must include names and contact information of the respective clients so that MPAO can contact and verify the project summaries.

1.6 Team Composition: It is expected that the proposer will maintain the required technical team as deemed as suited based on the requirements and milestones. However MPAO expects that the proposer would have allocated the following more team compositions having specific skill sets and professional experience. Importantly it is expected that the Proposer will maintain necessary resources on-site during crucial stages of the Project that requires closer interaction with MPAO during installation, configuration, training,

testing, etc.

Therefore the Proposer MUST provide the CVs of the following core team.

1.6.1 **Project Manager / Team Leader (one)**

- Five or more years of professional experience in executing large and complex IT projects.
- Demonstrated successful experience working as Team Leader / Project Manager in 2-3 previous projects of similar size and nature.
- Professional certificate is an asset.

1.6.2 **System Engineer / Security Administrator (one)**

Five or more years of professional experience in working as a system engineer or security administrator or related field, in large and complex projects.

1.7 Work Plan: Based on the technical specification and bill of materials, the Proposer should provide a detailed work plan for supply, delivery, installation, configuration, training and implementation of the proposed software and servers.

1.8 Minimum eligibility criteria: The proposer MUST comply the following minimum criteria. The Bid Document shall be rejected if it fails to meet the following minimum criteria and submit the require documents.

1.8.1 The proposer must have been in operation for at least **five years** in related to Supply, configuration and commissioning of IT equipment. The proposer shall submit the following document(s) for reference.

- Operational Certificate, or
- Contractual agreements, or
- Client testimonials
- Or any other document that clearly substantiate the compliance

1.8.2 The proposer MUST have at least five full time IT professionals under its payroll. The proposer shall submit the following documents.

- Organization structure
- Company Profile
- CVs of IT professionals

1.8.3 Must submit manufacturer authorization letter of the proposed equipment.

1.9 Evaluation Criteria: The evaluation shall be carried out only for Proposers that fully complies the minimum eligibility criteria as described above.

1.4.1	**Overall proposal presentation**	**5**
	Understanding of TOR / requirements	2
	Approach and Methodology / work plan and schedule	3
1.4.2	**Experience in supply of related equipment**	**15**
	(a) Supply record of proposed Firewalls	**10**

	i. Single organization	3
	ii. Two to Three organization	5
	iii. Four to five organization	7
	iv. More than five organization	10
	v. Supply of equipment other than proposed equipment in Single or more organization	3
	(b) Supply record of proposed Switches	**5**
	i. Single organization	1
	ii. Two to Three organization	2
	iii. Four to five organization	4
	iv. More than five organization	5
	v. Supply of software other than proposed software in Single or more organization	1
1.4.3	**Personnel CVs**	**12**
	(a) Project Manager / Team Leader (Number of CVs to be evaluated = 1)	**5**
	i. Qualification	**2**
	1. Masters or equivalent or higher	2
	2. Bachelors or equivalent	1
	ii. Experience	**2**
	1. One to three years of professional experience working as the System Engineer / Administrator or worked in related projects	1
	2. More than three years of professional experience working as the System Engineer / Administrator or worked in related projects	2
	III. Certification	**1**
	1. Any relevant certification	1
	(b) System Engineer / Security Administrator (Number of CVs to be evaluated = 1)	**7**
	I. Qualification	**2**
	1. Masters or equivalent in ICT or higher	2
	2. Bachelors or equivalent in ICT	1
	II. Experience	**2**
	1. One or three years of professional experience working as the System Engineer / Administrator or worked in related projects	1
	2. More than six years of professional experience working as the System Engineer / Administrator or worked in	2

	related projects	
	III. Certification	**3**
	1. Training Certification from the Manufacturer	3
	2. Any relevant IT certification	1
1.4.4	**Functionality and features of the proposed equipment.**	**30**
1.4.5	**Cost**	**30**
1.4.6	**Support**	**8**
	i. 24/7 support	8
	ii. Support within 24 hours	6
	iii. Support within 48 hours	4
	iv. Support within 1 week	2
	v. No support	0

1.10 Proposals shall be evaluated by an MPAO evaluation Committee.

1.11 MPAO has rights to update contents of RFP, even after publishing on the website. Proposers will be notified in writing of any change in the specifications contained in this Request for Proposal (RFP).

1.12 No verbal or written information which is obtained other than through this RFP or its addenda shall be binding on MPAO. No employee of MPAO is authorized to interpret any portion of this RFP in addition to that contained in or amended to this written RFP document.

1.13 **Right of Rejection and Clarification:** MPAO reserves the right to reject any and all proposals and to request clarification of information from any proposer. MPAO is not obliged to enter into a contract on the basis of any proposal submitted in response to this document.

1.14 **Request for Additional Information:** Prior to the final selection, proposer may be required to submit additional information which the MPAO may deem necessary to further evaluate proposer's qualifications.

1.15 MPAO will not reimburse proposers for any costs associated with the preparation and submittal of any proposal that are incurred.

1.16 Firewalls and Switches will be installed at MPAO server room. Rack space, UPS and cabling will be provided by MPAO.

1.17 **Right of Negotiation:** MPAO reserves the right to negotiate with the selected proposer the exact terms and conditions of the Contract.

1.18 MPAO is under no obligation to award this project to the proposer offering the lowest fee proposal. Evaluation criteria included in this document shall be used in the evaluating proposals.

1.19 **Exceptions to the RFP:** Proposer may find instances where they must take exception with certain requirements or specifications of the RFP. All exceptions shall be clearly identified, and written explanations shall include the scope of the exceptions, the ramifications of the exceptions for the MPAO, and a description of the advantage to be gained or disadvantages to be incurred by the MPAO as a result of these exceptions.

1.20 **Rights to Submitted Material:** All proposals, responses, inquiries, or correspondence relating to or in reference to this RFP, and all reports, charts, and other documentation submitted by proposer shall become the property of the MPAO when received.

1.21 **Contacts:** Proposers must submit proposals in accordance with the instructions contained in this RFP. If not MPAO has rights to disqualify such proposals. Questions regarding this request for proposal should be directed to:

admin@pension.gov.mv

1.22 **Submission of Bid:** Proposals must be delivered to the Maldives Pension Administration Office located at Ameenee Magu (next to Ministry of Finance) by **1500** hours on **26th November 2012**, at which time all bids will be privately opened.

1.23 **Contract:** The contract between MPAO and the proposer shall consist of

1.23.1 The RFP and any amendments thereto.

1.23.2 The proposal submitted.

1.24 **Termination of Contract**: MPAO may cancel the contract at any time for breach of contractual obligations by providing the Proposer with a written notice of such cancellation. Should the MPAO exercise its right to cancel the contract for such reasons, the cancellation shall become effective on the date as specified in the notice of cancellation sent to the contractor.

1.25 **Delivery and Installation:** All equipments should be delivered, installed and tested within 30 days after the signing of the contract. If fails to complete, MPAO has rights to deduct up to 1% per day from the available total cost, up to 15% of the whole project cost.

1.26 **Training:** At least 3 MPAO technical staffs should be trained from vendor certified training agency, before delivering the products.

1.27 **Warranty and maintenance:** All hardware and software should have minimum three years warranty period. During the warranty period, provider should check the system once in every three months and provide replacement for any defective. System provider should identify two support staffs, for MPAO to contact in case of any technical

assistance needed. Any problem reported to should be resolved within 48 hours.

1.28 Payment: Payment will be made within 20 days after completion of MPAO acceptance.

SECTION II

2.0 Technical Specifications

The following outlines the technical specifications of the required equipment and other software. The Proposer must clearly mention whether it meets the specification in 'Yes' or 'No'. The Proposals shall be considered no responsive if the following are not dully filled.

2.1 Firewall

Manufacturer: [Proposer to complete]			
Brand Name: [Proposer to complete]			
Model Number: [Proposer to complete]			
Quantity of Supply: Two			
General Requirements			
SN	**Features**	**Compliance**	**Remarks**
1	Firewall Should be Hardware Appliance base and high availability		
2	The Firewall should support stateful packet inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.		
3	The Firewall should be ICSA Labs certified for ICSA 4.0.		
4	The Firewall should support integration with any existing security infrastructure as per OPSEC standards.		
5	Licensing should be a per device and not user/IP based (should support unlimited users)		
6	Firewall Architecture should be on multiple tiers (firewall module, logging & policy management server, and the GUI/WebUI Console)		
7	The communication between all the components of Firewall System (firewall module, logging & policy management server, and the GUI/WebUI Console) should be encrypted with SSL or PKI.		
8	The firewall should be supplied with the support for RIP v2, OSPF & BGP routing protocols		
9	The firewall system should have the bandwidth management functionality.		
10	The firewall system should have the SSL VPN functionality which capable of handling 50 concurrent SSL VPN users.		
11	Should be able to do Data Leak Prevention in future.		
12	Should include the 3 Years comprehensive support.		
Interface and Connectivity Requirements			
SN	**Features**	**Compliance**	**Remarks**
1	The platform must be supplied with minimum 8 no of 10/100/1000Mbps Copper interfaces and 1 Console Interface. Should have LED and LCD's indicating Appliance Status.		
2	The platform should support VLAN tagging (IEEE 802.1q)		
3	The firewall should support ISP link load sharing		
Technical Requirements			
SN	**Features**	**Compliance**	**Remarks**

1	Stateful Inspection Firewall.		
2	Support a minimum of 1024 VLAN's.		
3	Integrated Multi site management.		
4	Built in storage capacity of 250GB minimum for storing logs.		
5	Power Input of 100 – 230V (50-60Hz).		
6	The box should be capable of upgrading to new versions/products in case a new feature is released by the OEM.		
7	Blocks attacks such as DoS, port scanning, IP/ICMP/TCP-related		
8	Encryption support of AES 128-256 bit, 3DES 56-168 bit		
9	Password, RADIUS, TACACS, X.509, Secure-ID authentication methods		
10	Integrated certificate authority (X.509)		
12	Should support star & mesh topology for VPN usage		
13	Should support an integrated IPS		
14	IPS should be capable a software fail open functionality in case of firewall performance going down.		
15	Should support unlimited policies.		
Performance Requirements			
SN	**Features**	**Compliance**	**Remarks**
1	The Firewall must support at least one million concurrent connections.		
2	The Firewall must support at least 100000 new sessions per second processing.		
3	The Firewall should support up to 3 Gbps of Firewall Throughput		
4	The appliance should support integrated IPS throughputs of minimum 2 Gbps		
5	Appliance should have a minimum IPSEC VPN throughput of up to 1 Gbps		
6	The unit should have a management module capable to manage multiple sites in future for centralized management during expansion.		
Firewall Filtering Requirements			
SN	**Features**	**Compliance**	**Remarks**
1	The Firewall should also support the standard Layer 3 mode of configuration with Interface IP's. It should be possible to protect the firewall policies from being compromised.		
2	The Firewall must provide NAT functionality, including dynamic and static NAT translations		
3	The Firewall must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type		
4	The Firewall should be able to filter traffic even if the packets are fragmented.		
5	Internet based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, MS-Exchange etc		
6	The Firewall should support authentication protocols like LDAP, RADIUS and have support for firewall passwords, smart cards, & token-based products like Secure ID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, and X.509 digital certificates.		
7	The Firewall should support database related filtering and should have support for Oracle and MSSQL.		
8	The Firewall should provide advanced NAT capabilities, supporting all applications and services-including H.323 and SIP based applications		
9	Support for Filtering TCP based applications		
10	Support basic inspection by working as a proxy for HTTP, FTP & SMTP traffic		
11	Support for Filtering incoming and outgoing e-mail based on		

	size and filters.		
12	Should support CLI & GUI based access to the firewall modules		
13	Local access to firewall modules should support role based access		
14	Local access to the firewall modules should support authentication protocols – RADIUS & TACACS+		
15	Firewall should have an integrated IPS capable of fail open option on failure & over load to ensure firewall availability.		
16	Integrated IPS should support hybrid attack detection/prevention with multiple attack protections methods, like Protocol Anomaly, Signature-Based, Day-Zero Protection, etc		
17	Integrated IPS should protect setup against vulnerabilities in the applications of the protected systems by carrying out deep packet inspection		
18	Should be able to protect against Malware and Bot Attacks if required		
19	Dedicated protection for web servers.		
Firewall Logging, Statistics and Reporting Requirements			
SN	**Features**	**Compliance**	**Remarks**
1	The Firewall must be able to send log information to an external log server via an encrypted connection		
2	The Firewall administration software must provide a means of viewing, filtering and managing the log data		
3	The Firewall logs must contain information about the firewall policy rule that triggered the log		
4	The Firewall must provide at a minimum basic statistics about the health of the firewall and the amount of traffic traversing the firewall		
5	Support to log in detail all connections which are blocked		
6	Support to log in detail all connections which go through the Firewall		
7	Provision to report all denied connections inbound		
8	Provision to report all denied connections outbound		
9	Provision to report all successful connections inbound		
10	Provision to report all successful connections outbound		
11	Provision to report traffic levels for inbound & outbound destinations		
12	Support to generate performance statistics on real-time basis		
13	Capability to produce reports which measure usage		
URL Filtering Requirements			
SN	**Features**	**Compliance**	**Remarks**
1	Should support both category base and Policy base URL filtering.		
3	White listing based on IP's & URL's.		
4	Black listing based on IP's & URL's.		
5	Exceptions based on network objects defined.		
6	Notification of Custom messages or URL redirection.		
7	Should provide Centralized, daily updates.		
Intrusion Prevention System			
SN	**Features**	**Compliance**	**Remarks**
1	Blocks attacks such as DoS, port scanning, IP/ICMP/TCP-related		
2	Blocks attacks such as DNS cache poisoning, FTP bounce, improper commands		
3	Signature-based, behavioral, and protocol anomaly		
4	IPS should be an integrated system with firewall		
5	IPS should have an option to run in by-pass mode if the CPU of the device increases		

Anti-Virus			
SN	**Features**	**Compliance**	**Remarks**
1	Protects HTTP, FTP, POP3, and SMTP		
2	Pattern-based spyware blocking at the gateway		
3	Centralized, daily updates, automatic and manual updates.		
4	File-based AV or protocol-based		

Anti-Spam			
SN	**Features**	**Compliance**	**Remarks**
1	Blocks spam and malware at the connection level by checking the sender's reputation against a dynamic database of known malicious IP addresses		
2	Protects against advanced forms of spam, including image-based and foreign-language spam, using pattern-based detection		
3	Utilizes block or allow lists to deny obvious email offenders and allow trusted senders		
4	Protects against a wide range of viruses and malware, including scans of message content and attachments		
5	Defends against new spam and malware outbreaks by using and distributing analysis engine		

Application Control			
SN	**Features**	**Compliance**	**Remarks**
1	The gateway should have feature to Identify, allow, block or limit usage of applications beyond ports and protocols.		
2	The solution should provide protection against the increasing threat vectors and malware introduced by internet applications.		
3	The solution should provide user interactive technology simplifying application control by asking and educating users in real time about Web 2.0 risks, policies and usage.		

Administration / Management Requirements			
SN	**Features**	**Compliance**	**Remarks**
1	Dedicated management system and real-time logs system should be provided		
2	The firewall management system must be capable of pushing firewall security policies and configurations to individual or multiple firewalls through a secure, encrypted connection interfaces		
3	The Firewall must provide simplified provisioning for addition of new firewalls where by a standard firewall policy could be pushed into the new firewall		
5	Any changes or commands issued by an authenticated user should be logged to a database.		
6	The Firewall must send SNMP traps to Network Management Servers (NMS) in response to System failures.		
7	Provision to generate automatic mail alerts		
8	Provision to send alerts to multiple recipients		
9	The Firewall must not support any non-secure means of access to the Firewall.		

User Authentication Requirements			
SN	**Features**	**Compliance**	**Remarks**
1	Support for user authentication at the firewall system for the different TCP/IP applications, like HTTP, SMTP, Telnet & RSH		
2	Support for integration with the RSA Secure ID as the strong user authentication mode		
3	Should be able to Integrate with AD or LDAP server for User base Authentication and User Base Policy enforcement.		

User Identity and Application Control			
SN	**Features**	**Compliance**	**Remarks**
1	Should have integrated Identity Control		
2	Should have integrated Application Control		
3	Should support User based Policies		
4	Should support User Machine awareness		
5	Time based polices		
6	Should support Clientless and agent less authentication		
7	Should have portal base authentication		
8	Identity agent based authentication		
11	Application based logs		
12	User based logs		
13	Should support user check based feature which would document user decision on he has to access an application		
14	Should support bandwidth allocation based on applications		

2.2 Core Switches

Manufacturer: [Proposer to complete]			
Brand Name: [Proposer to complete]			
Model Number: [Proposer to complete]			
Quantity of Supply: Four			
General Requirements			
SN	**Features**	**Compliance**	**Remarks**
1	Multilayer switching		
2	24 10/100/1000 auto sensing Gigabit Ethernet switching ports.		
3	Auto negotiation for speed, duplex mode and flow control.		
4	Media Access Control Security hardware-based encryption		
5	IPv4 and IPv6 routing, Multicast routing, advanced quality of service (QoS), and security features in hardware		
6	Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall systems performance.		
7	Up to 1024 VLAN support		
8	Must have at least 256MB SDRAM.		
9	Must have at least 32MB of flash memory.		
10	Should provide enterprise level performance		
11	Rack mountable		
Switch Administration and Management			
SN	**Features**	**Compliance**	**Remarks**
1	Configuration management		
2	Event notification		
3	Task-based menu		
4	File management		
5	OS Software upgrades		

Thank You

19-11-2012