TENDER DOCUMENT FOR

SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF FIREWALL

NATIONAL CENTRE FOR ANTARCTIC & OCEAN RESEARCH
(Ministry of Earth Sciences, Govt. Of India)
Headland Sada, Vasco-da-Gama
GOA -403 804, INDIA
Tel: 91- (0) 832 2525571 TeleFax: 91- (0) 832 2525573
Email: warlu62@ncaor.gov.in
Website: www.ncaor.gov.in

NATIONAL CENTRE FOR ANTARCTIC & OCEAN RESEARCH
(*Ministry of Earth Sciences, Govt. Of India*),
HEADLAND SADA, VASCO-DA-GAMA, GOA - 403 804

TENDER NO. NCAOR/PR-1199/PT-35
TENDER FOR SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL.

1.	**SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL** **Quantity-** **Specification-**	 01 As per Annexure I
2.	General Terms and Conditions	As per Annexure II
3.	Cost of Tender Documents (In Person)	` 500.00
4.	Cost of Tender Documents (By Post)	` 550.00
5.	EMD	**Tender documents can be downloaded by tenderers from NCAOR website. In case a tenderer is using the documents and forms downloaded from the website, the cost of tender documents shall be sent in the form of Bank Draft in a separate envelope along with the tender.** **Bidders** shall submit **EMD** along with their tender, either by DD drawn in favor of NCAOR, for a sum of ` 15,000.00 (Rupees Fifteen Thousand only) payable at Vasco-da-Gama only. **Or** **In the form of a bank guarantee** for a sum of ` 15,000.00 (Rupees Fifteen Thousand only)
6.	Last Date and time for issue of tender documents	**MONDAY** **20.10.2014** 1600 Hrs (IST)
7.	Last Date and time for submission of sealed quotations	**TUESDAY** **21.10.2014** 1700Hrs (IST)
8.	Date and time of tender opening	**WEDNESDAY** **22.10.2014** 1000Hrs (IST)

ANNEXURE – I

SPECIFICATION FOR SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL.

	Name of the Item or Related Service : Technical Specification and Standards for UTM/NGFW (Firewall)
Sl. No.	**Specification**
1	The Firewall must be appliance based and should facilitate multi-application environment.
2	The Firewall should be ICSA Labs certified for ICSA 4.0 and EAL 4 certified, if not the same model
3	The platform should be based on realtime, secure embedded operating system
4	Should support minimum 8 virtual firewall or more
5	The proposed system shall support unlimited IP/User license for Firewall / VPN (IPSec & SSL)/ IPS/WCF/AV
6	Should provide a Http, Https, SSH, Telnet, SNMP based management console for managing and configuring various components of the appliance
7	The device should belong to a family of products that attains NSS Approved (UTM) Certification
8	The device should belong to a family of products that attains IPv6 Ready Phase 2 & IPv6 Certification
9	Proposed Firewall Vendor should be in the Leaders' Quadrant of Gartner Magic Quadrant for the last 3 consecutive years in UTM.
10	The OEM must attain ISO 9001:2000 certification that covers scope of the Quality Management System which includes the design, development and manufacturing of network security products and the delivery of associated security services and support
11	OEM should have direct technical support centre in India.
12	OEM should have direct RMA Centre in India for Hardware Warranty.
13	OEM should have direct product training facility with certified trainer in India. And should provide training to Tow person of organization along with product certification.
14	The Firewall Appliance should be rack mountable and shall not exceeding 2U
B.	**Networking & System Performance Requirements:**
1	The Firewall should support a minimum of 6 x 10/100/1000 interfaces & 4 X 10/100/1000 SFP Fiber Interface with auto sensing capacity
2	The platform should support the standards based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.
3	The Firewall should support IEEE 802.1q VLAN Tagging with about 1024 VLANs supported (in NAT/Route mode)
4	Should support automatic ISP failover as well as ISP load sharing for outbound traffic
5	The Firewall should support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS, RIPng
6	The Firewall should support Static, Policy Based, and Multicast routing
7	The Firewall should support throughputs of 8 Gbps or better for both small & large packets
8	The firewall should support throughput of atleast 7 Gbps of AES - IPSEC VPN
9	should support concurrent session atleast 6 Million
10	Should support new session per second atleast 2,00,000

11	Should support and IPS throughput of 2.8 Gbps or better
12	Should support and GAV throughput of upto 2.5 Mbps
13	Should support Site to Site VPN Tunnels up to 2,000
14	Should support Client to Site VPN Tunnels up to 10,000
15	Should support firewall Policies up to 10,000
16	Should support End Point Protation Client up to 600
17	Should support Access Point Centralize Management up to 512 AP
18	Should support Two Factor Authentication Token up to 1000
C.	**Operating System & Management Requirements:**
1	Be proprietary to prevent inheriting common OS vulnerabilities
2	Resided on flash disk for reliability over hard disk
3	Allow multiple OS firmware image for booting options
4	Upgradeable via Web UI or TFTP
5	Be easily backup or restored via GUI and CLI to/from local PC, remote centralized management or USB disk
6	The system shall support profile base login account administration, offering gradual access control such as only to Policy Configuration & Log Data Access
7	The proposed system shall be able to limit remote management access from certain trusted network or host with corresponding administrator account
8	The proposed system should be able to facilitate administration audits by logging detailed activities to event log for management & configuration updates
9	The administrator authentication shall be facilitated by local database, PKI & remote services such as Radius, LDAP and TACAS+
10	The Firewall must be capable of clustering multiple firewalls together into a redundant and highly available stateful configuration without any extra license cost for creating HA.
D.	**Firewall Requirements:**
1	The Firewall should support deployement modes as; “Stealth Mode” or “Route Mode" or "Transparent Mode” or "Proxy Mode".
2	The proposed system should have integrated Traffic Shaping / QoS functionality
4	Should support DHCP server & DHCP Agent functionality
5	The Firewall should support Stateful inspection with optional Policy based NAT (Static OR Dynamic)
6	The Firewall should support Inbound Port Forwarding with optional inbound Load Balancing
7	Should support IPv6 ACL to implement security Policy for IPv6 traffic
8	All internet based applications should be supported for filtering like Telnet, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, BGP, IMAP, NFS etc
9	Should be able to inspect HTTP and FTP traffic when these are deployed using non standard port(i.e when HTTP is not using standard port TCP/80)
E.	**High Availability Requirements:**
1	The firewall must support Active-Active as well as Active-Passive redundancy.
2	The Firewall must support stateful clustering of multiple active firewalls, and the firewalls must load balance the traffic between them to share the load.
3	The cluster should support simple and minimal downtime during upgrade
F.	**IPSEC VPN Requirements:**
1	The IPSEC VPN and SSL VPN capability shall minimally attain Internet Computer Security Association (ICSA) Certification or equivalent

2	The proposed system shall comply/support industry standards, L2TP, PPTP, IPSEC, and SSL VPN without additional external solution, hardware or modules:
3	The device shall utilize inbuilt hardware VPN acceleration supported for:
3.1	IPSEC (DES, 3DES, AES) encryption/decryption
3.2	SSL encryption/decryption
4	The system shall support the following IPSEC VPN capabilities:
4.1	Multi-zone VPN supports.
4.2	IPSec, ESP security.
4.3	Supports Aggressive and Dynamic mode
4.4	Support perfect forward secrecy group 1 and group 2 configuration
4.5	MD5 or SHA1 authentication and data integrity.
4.6	Automatic IKE (Internet Key Exchange) and Manual key exchange.
4.7	Supports NAT traversal
4.8	Supports Extended Authentication
4.9	Supports Hub and Spoke architecture
4.10	Supports Redundant gateway architecture
4.11	DDNS support
G.	**SSL VPN Requirements:**
1	The Firewall should be integrated solution and there should be no user based licensing for SSL VPN.
2	The Firewall should support for TWO modes of SSL VPN:
2.1	Web-only mode: for thin remote clients equipped with a web browser only and support web application such as:HTTP/HTTPS PROXY, FTP, SMB/CIFS, SSH, VNC, RDP
2.2	Tunnel mode, for remote computers that run a variety of client and server applications
4	The system shall provide SSL VPN tunnel mode that supports 32 and 64-bit Windows operating systems
5	The proposed solution shall allow administrators to create multiple bookmarks to add to a group and make these bookmarks available for SSL-VPN users.
H.	**Network Intrusion Detection & Prevention System Requirements:**
1	The IPS capability shall minimally attain Internet Computer Security Association (ICSA) NIPS or NSS Certification
2	Should have a built-in Signature and Anomaly based IPS engine on the same unit
3	Able to prevent denial of service and Distributed Denial of Service attacks.
4	Signature based detection using real time updated database
5	The device shall allow administrators to create Custom IPS signatures
6	Configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types.
7	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)
8	Security check updates do not require reboot of the unit.
9	Supports attack recognition inside IPv6 encapsulated packets.
10	Supports user-defined signatures with Regular Expressions.
11	Supports several prevention techniques including drop-packet, tcp-rst (Client, Server & both) etc. List all prevention options
12	SSL Inspection for IPS
I.	**Antivirus System Requirements:**

1	The Antivirus capability shall minimally attain Internet Computer Security Association (ICSA)/equivalent AV Certification
2	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy
3	The System should be able to scan following Protocols:
3.1	HTTP and HTTPS
3.2	SMTP, SMTPS
3.3	FTP, FTPS
3.4	POP3, POP3S
3.5	IMAP, IMAPS
3.6	Instant Messenger (AIM, YAHOO!, MSN, ICQ, SIMPLE)
3.7	NNTP
4	The proposed system shall provide ability to allow, block and intercept (allow but quarantine) attachments or downloads according to file extensions and/or file types
5	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.
6	The solution should be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus
J.	**Web & Application Content Filtering System Requirements:**
1	The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.
2	URL database should have atleast 40 million + sites and 75 + categories.
3	The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.
4	Should blocks web plug-ins such as ActiveX, Java Applet, and Cookies.
5	Shall include Web URL block
6	Shall include Web Exempt List
7	The proposed solution should be able to replace the web page when the web page matches the Web Filtering blocking criteria.
8	The proposed solution shall be able to identify, retrieve and rate the actual URL of the cache content commonly available in search engines such as Yahoo and Google.
9	The solution shall allow administrators to creat mutiple new local URL filtering categories besides dynamic categories
10	Should have application control feature
11	Should have the intelligance to identify & control of popular IM & P2P applications like KaZaa,BitTorrent etc.
12	Should have minimum database of 3300 types of application awareness
K.	**Data Leak Prevention Requirements:**
1	Should have the ablity to prevent data loss through SMTP, SMTPS, FTP, HTTP, HTTPS & IM
2	Should have built in pattern database
L	**User Authentication**
1	The proposed Firewall shall be able to support various form of user Authentication methods simultaneously , including:
2	Local Database entries
3	LDAP server entries
4	RADIUS server entries

5	TACACS+ server entries
6	Native Windows AD (Single sign on capability)
7	Two-factor authentication without any external Hardware.
8	Citrix Agent support for Single Sign On
10	The solution shall be capable of providing Windows AD single sign-on by means of collector agents which broker between users when they log on to the AD domain and the device.
11	The proposed appliance shall support inbuilt 2 factor authentication services and database using tokens, email and SMS.Hardware Token supported should be 1000. If this service is not available on the box, provide an external server for authentication.
12	System should also have capability to identify devices (ex. Android, Iphone, Windows etc) & should be able to write policies on basis of device identity
13	Should also support Authentication-based routing
M	**Wireless Security**
1	Integrated wireless Controller support required & Number of Managable Wireless accespoints support required
2	Wireless Security features like WEP,WPA-PSK & WPA-ENT should be supported
3	Should have a inbuilt DHCP Server to assign IP Addresses to specific SSID's and should support DHCP Relay
4	Should have ability to detect wireless as well as on-wire rogue AP
5	Total number of AP's supported 512
6	Should support on-box Guest Management Feature
7	Administrators shall be able to setup per SSID, a MAC address filter list to either permit or exclude a list of clients identified by their MAC addresses.
8	Administrators shall be able to view client monitor which illustrate wireless access situation
9	Wireless Deployment should support wired AP's i.e AP's connected on LAN as well as Wireless Bridged AP's i.e AP's connected by Wireless backhaul.
10	Should support Wireless IDS for following types of intrusion detection among others:
11	1.1 Unauthorized Device Detection
12	1.2 Rogue/Interfering AP Detection
13	1.3 Adhoc Network Detection and Containment
14	1.4 Wireless Bridge Detection
15	1.5 Misconfigured AP Detection
16	1.6 Weak WEP Detection
17	1.7 Multi Tenancy Protection
18	1.8 MAC OUI Checking
N	**BYOD**
1	create policies based on device type
2	identify and monitor the types of devices connecting to your networks, wireless or wired
3	use MAC address based access control to allow or deny individual devices
4	enforce endpoint control on devices that can run Client Endpoint Control software
O	**Client Reputation**
1	Should be able to provide information by tracking client behavior and reporting on the activities you determine are risky or otherwise noteworthy.
2	Bad Connection Attempts
3	Packets that are blocked by deny security policies.
4	Intrusion Protection
5	Malware Protection

6	Web Activity
7	Application Protection
8	Geographical locations that clients are communicating with.
P	**End Point Protection**
1	The solution should have Anti virus, Web filtering, Application control,IPSec & SSL VPN, vulnerability scan etc features.
2	The solution should have VB100 certification
3	The solution should support Android & iOS along with Windows & MAC
4	Should be managed from a single console
5	Can be deployed in the network through Active Directory
6	Should have the feature of rootkit removal
7	Should identify system & application vulnerability
8	Should have the application firewall protection to block any specific application
9	Should have the option of creating customized MSI installer package
10	The software should support windows XP or higher
11	Should have the quarentine feature
12	The solution can work standalone or centrally managed
13	Should have the client certificate support
Q	**Support and Warranty**
1	Should have 24X7 Warranty and Support from OEM for Product Hardware and Firmware/OS
R	**License**
1	Commercial Need to be quote for Three Years 24X7 Fully Bundle Hardware Appliance and Features as per above specification. (Exp. Gateway Antivirus, spyware, web/url filtering, content and application filtering, SSL VPN & IPS) all Hardware Component and Licenses should be installed from day one and License period will be counted from date of activation.

TECHNICAL COMPLIANCE STATEMENT FOR SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL.

Name of the Item or Related Service : Technical Specification and Standards for UTM/NGFW (Firewall)			
Sl. No.	**Specification**	**COMPLIED /NOT COMPLIED**	**EXTRA FEATURES**
1	The Firewall must be appliance based and should facilitate multi-application environment.		
2	The Firewall should be ICSA Labs certified for ICSA 4.0 and EAL 4 certified, if not the same model		
3	The platform should be based on realtime, secure embedded operating system		
4	Should support minimum 8 virtual firewall or more		
5	The proposed system shall support unlimited IP/User license for Firewall / VPN (IPSec & SSL)/ IPS/WCF/AV		
6	Should provide a Http, Https, SSH, Telnet, SNMP based management console for managing and configuring various components of the appliance		
7	The device should belong to a family of products that attains NSS Approved (UTM) Certification		
8	The device should belong to a family of products that attains IPv6 Ready Phase 2 & IPv6 Certification		
9	Proposed Firewall Vendor should be in the Leaders' Quadrant of Gartner Magic Quadrant for the last 3 consecutive years in UTM.		
10	The OEM must attain ISO 9001:2000 certification that covers scope of the Quality Management System which includes the design, development and manufacturing of network security products and the delivery of associated security services and support		
11	OEM should have direct technical support centre in India.		
12	OEM should have direct RMA Centre in India for Hardware Warranty.		
13	OEM should have direct product training facility with certified trainer in India. And should provide training to Tow person of organization along with product certification.		
14	The Firewall Appliance should be rack mountable and shall not exceeding 2U		
B.	**Networking & System Performance Requirements:**		
1	The Firewall should support a minimum of 6 x 10/100/1000 interfaces & 4 X 10/100/1000 SFP Fiber Interface with auto sensing capacity		
2	The platform should support the standards based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.		
3	The Firewall should support IEEE 802.1q VLAN Tagging with about 1024 VLANs supported (in NAT/Route mode)		
4	Should support automatic ISP failover as well as ISP load sharing for outbound traffic		

5	The Firewall should support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS, RIPng		
6	The Firewall should support Static, Policy Based, and Multicast routing		
7	The Firewall should support throughputs of 8 Gbps or better for both small & large packets		
8	The firewall should support throughput of atleast 7 Gbps of AES - IPSEC VPN		
9	should support concurrent session atleast 6 Million		
10	Should support new session per second atleast 2,00,000		
11	Should support and IPS throughput of 2.8 Gbps or better		
12	Should support and GAV throughput of upto 2.5 Mbps		
13	Should support Site to Site VPN Tunnels up to 2,000		
14	Should support Client to Site VPN Tunnels up to 10,000		
15	Should support firewall Policies up to 10,000		
16	Should support End Point Protation Client up to 600		
17	Should support Access Point Centralize Management up to 512 AP		
18	Should support Two Factor Authentication Token up to 1000		
C.	**Operating System & Management Requirements:**		
1	Be proprietary to prevent inheriting common OS vulnerabilities		
2	Resided on flash disk for reliability over hard disk		
3	Allow multiple OS firmware image for booting options		
4	Upgradeable via Web UI or TFTP		
5	Be easily backup or restored via GUI and CLI to/from local PC, remote centralized management or USB disk		
6	The system shall support profile base login account administration, offering gradual access control such as only to Policy Configuration & Log Data Access		
7	The proposed system shall be able to limit remote management access from certain trusted network or host with corresponding administrator account		
8	The proposed system should be able to facilitate administration audits by logging detailed activities to event log for management & configuration updates		
9	The administrator authentication shall be facilitated by local database, PKI & remote services such as Radius, LDAP and TACAS+		
10	The Firewall must be capable of clustering multiple firewalls together into a redundant and highly available stateful configuration without any extra license cost for creating HA.		
D.	**Firewall Requirements:**		
1	The Firewall should support deployement modes as; “Stealth Mode” or “Route Mode" or "Transparent Mode” or "Proxy Mode".		
2	The proposed system should have integrated Traffic Shaping / QoS functionality		
4	Should support DHCP server & DHCP Agent functionality		
5	The Firewall should support Stateful inspection with optional Policy based NAT (Static OR Dynamic)		

6	The Firewall should support Inbound Port Forwarding with optional inbound Load Balancing		
7	Should support IPv6 ACL to implement security Policy for IPv6 traffic		
8	All internet based applications should be supported for filtering like Telnet, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, BGP, IMAP, NFS etc		
9	Should be able to inspect HTTP and FTP traffic when these are deployed using non standard port(i.e when HTTP is not using standard port TCP/80)		
E.	**High Availability Requirements:**		
1	The firewall must support Active-Active as well as Active-Passive redundancy.		
2	The Firewall must support stateful clustering of multiple active firewalls, and the firewalls must load balance the traffic between them to share the load.		
3	The cluster should support simple and minimal downtime during upgrade		
F.	**IPSEC VPN Requirements:**		
1	The IPSEC VPN and SSL VPN capability shall minimally attain Internet Computer Security Association (ICSA) Certification or equivalent		
2	The proposed system shall comply/support industry standards, L2TP, PPTP, IPSEC, and SSL VPN without additional external solution, hardware or modules:		
3	The device shall utilize inbuilt hardware VPN acceleration supported for:		
3.1	IPSEC (DES, 3DES, AES) encryption/decryption		
3.2	SSL encryption/decryption		
4	The system shall support the following IPSEC VPN capabilities:		
4.1	Multi-zone VPN supports.		
4.2	IPSec, ESP security.		
4.3	Supports Aggressive and Dynamic mode		
4.4	Support perfect forward secrecy group 1 and group 2 configuration		
4.5	MD5 or SHA1 authentication and data integrity.		
4.6	Automatic IKE (Internet Key Exchange) and Manual key exchange.		
4.7	Supports NAT traversal		
4.8	Supports Extended Authentication		
4.9	Supports Hub and Spoke architecture		
4.10	Supports Redundant gateway architecture		
4.11	DDNS support		
G.	**SSL VPN Requirements:**		
1	The Firewall should be integrated solution and there should be no user based licensing for SSL VPN.		
2	The Firewall should support for TWO modes of SSL VPN:		
2.1	Web-only mode: for thin remote clients equipped with a web browser only and support web application such		

	as:HTTP/HTTPS PROXY, FTP, SMB/CIFS, SSH, VNC, RDP		
2.2	Tunnel mode, for remote computers that run a variety of client and server applications		
4	The system shall provide SSL VPN tunnel mode that supports 32 and 64-bit Windows operating systems		
5	The proposed solution shall allow administrators to create multiple bookmarks to add to a group and make these bookmarks available for SSL-VPN users.		
H.	**Network Intrusion Detection & Prevention System Requirements:**		
1	The IPS capability shall minimally attain Internet Computer Security Association (ICSA) NIPS or NSS Certification		
2	Should have a built-in Signature and Anomaly based IPS engine on the same unit		
3	Able to prevent denial of service and Distributed Denial of Service attacks.		
4	Signature based detection using real time updated database		
5	The device shall allow administrators to create Custom IPS signatures		
6	Configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types.		
7	Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)		
8	Security check updates do not require reboot of the unit.		
9	Supports attack recognition inside IPv6 encapsulated packets.		
10	Supports user-defined signatures with Regular Expressions.		
11	Supports several prevention techniques including drop-packet, tcp-rst (Client, Server & both) etc. List all prevention options		
12	SSL Inspection for IPS		
I.	**Antivirus System Requirements:**		
1	The Antivirus capability shall minimally attain Internet Computer Security Association (ICSA)/equivalent AV Certification		
2	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy		
3	The System should be able to scan following Protocols:		
3.1	HTTP and HTTPS		
3.2	SMTP, SMTPS		
3.3	FTP, FTPS		
3.4	POP3, POP3S		
3.5	IMAP, IMAPS		
3.6	Instant Messenger (AIM, YAHOO!, MSN, ICQ, SIMPLE)		
3.7	NNTP		
4	The proposed system shall provide ability to allow, block and intercept (allow but quarantine) attachments or downloads according to file extensions and/or file types		

5	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.		
6	The solution should be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus		
J.	**Web & Application Content Filtering System Requirements:**		
1	The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.		
2	URL database should have atleast 40 million + sites and 75 + categories.		
3	The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.		
4	Should blocks web plug-ins such as ActiveX, Java Applet, and Cookies.		
5	Shall include Web URL block		
6	Shall include Web Exempt List		
7	The proposed solution should be able to replace the web page when the web page matches the Web Filtering blocking criteria.		
8	The proposed solution shall be able to identify, retrieve and rate the actual URL of the cache content commonly available in search engines such as Yahoo and Google.		
9	The solution shall allow administrators to creat mutiple new local URL filtering categories besides dynamic categories		
10	Should have application control feature		
11	Should have the intelligance to identify & control of popular IM & P2P applications like KaZaa,BitTorrent etc.		
12	Should have minimum database of 3300 types of application awareness		
K.	**Data Leak Prevention Requirements:**		
1	Should have the ablity to prevent data loss through SMTP, SMTPS, FTP, HTTP, HTTPS & IM		
2	Should have built in pattern database		
L	**User Authentication**		
1	The proposed Firewall shall be able to support various form of user Authentication methods simultaneously , including:		
2	Local Database entries		
3	LDAP server entries		
4	RADIUS server entries		
5	TACACS+ server entries		
6	Native Windows AD (Single sign on capability)		
7	Two-factor authentication without any external Hardware.		
8	Citrix Agent support for Single Sign On		
10	The solution shall be capable of providing Windows AD single sign-on by means of collector agents which broker between users when they log on to the AD domain and the device.		

11	The proposed appliance shall support inbuilt 2 factor authentication services and database using tokens, email and SMS.Hardware Token supported should be 1000. If this service is not available on the box, provide an external server for authentication.		
12	System should also have capability to identify devices (ex. Android, Iphone, Windows etc) & should be able to write policies on basis of device identity		
13	Should also support Authentication-based routing		
M	**Wireless Security**		
1	Integrated wireless Controller support required & Number of Managable Wireless accespoints support required		
2	Wireless Security features like WEP,WPA-PSK & WPA-ENT should be supported		
3	Should have a inbuilt DHCP Server to assign IP Addresses to specific SSID's and should support DHCP Relay		
4	Should have ability to detect wireless as well as on-wire rogue AP		
5	Total number of AP's supported 512		
6	Should support on-box Guest Management Feature		
7	Administrators shall be able to setup per SSID, a MAC address filter list to either permit or exclude a list of clients identified by their MAC addresses.		
8	Administrators shall be able to view client monitor which illustrate wireless access situation		
9	Wireless Deployment should support wired AP's i.e AP's connected on LAN as well as Wireless Bridged AP's i.e AP's connected by Wireless backhaul.		
10	Should support Wireless IDS for following types of intrusion detection among others:		
11	1.1 Unauthorized Device Detection		
12	1.2 Rogue/Interfering AP Detection		
13	1.3 Adhoc Network Detection and Containment		
14	1.4 Wireless Bridge Detection		
15	1.5 Misconfigured AP Detection		
16	1.6 Weak WEP Detection		
17	1.7 Multi Tenancy Protection		
18	1.8 MAC OUI Checking		
N	**BYOD**		
1	create policies based on device type		
2	identify and monitor the types of devices connecting to your networks, wireless or wired		
3	use MAC address based access control to allow or deny individual devices		
4	enforce endpoint control on devices that can run Client Endpoint Control software		
O	**Client Reputation**		
1	Should be able to provide information by tracking client behavior and reporting on the activities you determine are risky or otherwise noteworthy.		
2	Bad Connection Attempts		
3	Packets that are blocked by deny security policies.		

4	Intrusion Protection		
5	Malware Protection		
6	Web Activity		
7	Application Protection		
8	Geographical locations that clients are communicating with.		
P	**End Point Protection**		
1	The solution should have Anti virus, Web filtering, Application control, IPSec & SSL VPN, vulnerability scan etc features.		
2	The solution should have VB100 certification		
3	The solution should support Android & iOS along with Windows & MAC		
4	Should be managed from a single console		
5	Can be deployed in the network through Active Directory		
6	Should have the feature of rootkit removal		
7	Should identify system & application vulnerability		
8	Should have the application firewall protection to block any specific application		
9	Should have the option of creating customized MSI installer package		
10	The software should support windows XP or higher		
11	Should have the quarentine feature		
12	The solution can work standalone or centrally managed		
13	Should have the client certificate support		
Q	**Support and Warranty**		
1	Should have 24X7 Warranty and Support from OEM for Product Hardware and Firmware/OS		
R	**License**		
1	Commercial Need to be quote for Three Years 24X7 Fully Bundle Hardware Appliance and Features as per above specification. (Exp. Gateway Antivirus, spyware, web/url filtering, content and application filtering, SSL VPN & IPS) all Hardware Component and Licenses should be installed from day one and License period will be counted from date of activation.		

Annexure-II

TERMS AND CONDITIONS FOR SUBMISSION OF QUOTATION

1) The National Centre for Antarctic and Ocean Research (NCAOR) **invites sealed quotations in two-parts** from the reputed firms for the **"SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL**" at NCAOR, GOA as per the specifications given in Annexure I.

2**)** The technical and financial Bids should be submitted in two separate sealed covers, super scribing **"Part-I Technical Bid for "SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL" Tender No., due date and "Part-II Financial Bid for "SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL" Tender No., due date. Both the bids should be kept in a single cover by super scribing tender for "SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL"** sealed and addressed to the Director, National Centre for Antarctic and Ocean Research, Headland-Sada, Vasco-da-Gama, Goa-403 804. **Offer sent through fax will not be accepted.**

3) Overwriting and corrections should be attested properly. The bid should be complete in all respects and should be duly signed. Incomplete and unsigned bids will not be considered at all.

4) All relevant technical literature pertain to items quoted **with full specifications** (Drawing, if any), information about the products quoted, including brochures if any should accompany the quotation.

5) A list of **reputed clients** to whom the firm has supplied similar items to be furnished along-with the quotation.

In the TECHNICAL BID, the Bidder should furnish the Name and address of the Purchasers placed orders on similar equipment with order No, date, Description and quantity, Date of Supply alongwith Contact person Telephone No, Fax No, and e mail address of Purchaser.

The Bidder should enclose copies of Purchase Orders only in the FINANCIAL BID.

6) Quotation should be **valid for a period of 90 days** from the date of tender opening and the period of delivery required should also be clearly indicated. If the supplier fails to deliver the goods within the time to be agreed upon, for delayed deliveries and for delays in installation

(wherever applicable) NCAOR reserves the right to **levy liquidated damages** at the rate of 0.5% per week or part their of upto maximum of 5%.

7) Commissioning has to be completed within three months from the date of receipt of goods.

8) The **warranty period** and the kind of **post-warranty support** should be indicated. Warranty shall commence from the date of installation and acceptance of the complete equipment supplied under the Purchase Order / Contract.

9) **Technical bid should contain EMD.**

Bidders shall submit **EMD** along with their tender, **either By DD** drawn in favor of NCAOR, on any nationalized bank for a sum of ` 15,000/- (Rupees Fifteen Thousand only) payable at Vasco-da-Gama only **or in the form of a bank guarantee** for a sum of ` 15,000/- (Rupees Fifteen Thousand only) from any reputed bank (scheduled bank) initially valid for 180 days from the date of closing of the tender as per the proforma enclosed. This bank Guarantee in original shall be submitted along with the technical bid only.

Tender without EMD in the envelope containing technical bid shall be summarily rejected. The EMD of unsuccessful bidders shall be returned within 30 days of the award of contract.

The earnest money will be liable to be forfeited, if the tenderer withdraws or amends, impairs or derogates from the tender if any respect within the period of validity of his tender.

10) Please **specify the Make/Brand** and Name of the Manufacturer with address, country of origin and currency in which rates are quoted.

11) The Purchaser requires that the bidders suppliers and contractors observe the highest standard of ethics during the procurement and execution of such contracts. In pursuit of this policy, the following are defined:

“Corrupt practice” means the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of a public official in the procurement process or in contract execution:

"fradulent practice" means a misrepresentation or omission of facts in order to influence a procurement process or the execution of contract;

"collusive practice" means a scheme or arrangement between two or more bidders, with or without the knowledge of purchaser, designed to establish bid prices at artificial, noncompetitive levels; and

"coercive practice: means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the procurement process or affect the execution of contract;

The purchaser will reject a proposal for award if it determines that the Bidder recommended for award has, directly or through an agent, engaged in corrupt, fraudulent, collusive or coercive practices in competing for the contract in question; The Decision of Director, NCAOR shall be final and binding.

12) Bidders that doesn't manufacture the goods it offers to supply shall submit Manufacturer's Authorization form on the letterhead of the Manufacturer duly signed and stamped by a person with the proper authority to sign documents that are binding on the Manufacturer as per the following format should be submitted failing which the quotation will not be considered.

To
The Director
NCAOR
GOA

Sub: Manufacturers' Authorization form against Tender No:_____

We_____(Name of the Manufacturer) who are official manufacturers of _____(Type of goods manufactured) having factories at _____(full address of Manufacturer's factories) do hereby authorize _____(Name of the Bidder) to submit a bid against your Tender No._____for the _____Goods manufactured by us and to subsequently negotiate and sign the contract.

We hereby extend our full guarantee and warranty with respect to the Goods offered by the above firm

Manufacturer's Name:
Signature of Authorized
representative of the Manufacturer:

Duly authorized to sign this Authorization on behalf of : _____(Name of the Bidder)
Date:

In case the bidder not doing business within India, shall furnish the certificate to the effect that the bidder is or will be represented by an agent in India equipped and able to carry out the supply, maintenance, repair obligations etc., during the warranty and post warranty period or ensure a mechanism at place for carrying out the supply, maintenance, repair obligations etc., during the warranty and post- warranty period.

13) **The order acknowledgement** should be from the principals and if the Indian Agent is empowered to quote and to furnish order acknowledgement, a copy of agreement entered by you with the Indian Agent to be furnished.

14) **Compliance Statement:** Equipments point-by-point comparison/compliance statement with **technical specification** indicated in the tender, should be enclosed along with your tender as well as any other extra features of the equipment be shown separately therein and also **compliance statement for all commercial terms** of the tender document.

15) NCAOR is not entitled to issue form **"C/D**". No Sales Tax or any other Tax shall be payable by us unless payment of the same is specifically mentioned by the suppliers in their bids and same is legally leviable.

16) To avail duty concessions i.e. **Excise Duty** as per Govt. notification 10/97 & **Custom Duty** as per Govt. notification 51/96, NCAOR will provide exemption certificates. Hence, the rates should be split into basic cost and Excise Duty if any.

17) **Technical Bid should contain** all details and specifications of the equipment offered, delivery schedule, warranty, payment term, installation, training, post-warranty, user-list, service support **WITHOUT PRICE** and **Financial bid should contain** details of the price(s) of the item(s) quoted in the technical bid. The Technical bid should not contain any references to the pricing.

In case the technical bid contains any direct or indirect reference to quoted price the bid is liable to be rejected.

18) Submit your quote on F.O.R. destination basis. However tender should contain item-wise prices including total ex-works price, overall weight & dimensions of the equipment and cost of packing forwarding, approx. cost of freight charges for delivery up to Goa, India.

19) A Committee constituted by the Director, NCAOR for the purpose reserves the right to open the bids. Only technical bids will be opened on the date and time mentioned in the tender document. The financial bids of those tenderers whose technical bids are found to be meeting our specifications only will be opened in their presence at date and time to be notified later.

20) The firm to the full satisfaction of the NCAOR should carry out the **installation and commissioning** at the NCAOR premises and the time-frame for the whole process should be specified in the technical bid.

21) A technical Committee constituted by the Director will assess the product supplied/installed for their quality and their conformity to the specifications provided by the firm in their quotations. Any item(s) identified by the Committee to be not as per the specifications or are found to be of inferior quality will be rejected, and the bills towards the supply will not be processed for payment till proper replacements are provided.

22) **No advance payment** will be made. Payment shall be made after supply, installation and acceptance of the equipment by NCAOR. The payment will be authorized after submission of a Bank Guarantee for 10% value of the order towards warranty guarantee. The **performance Bank Guarantee** should be furnished within 15 days from the date of placement of order from a reputed bank (scheduled bank in India **or** foreign bank operating in India) valid till 60 days after the warranty period.

23) Suppliers should clearly define the mechanisms of **post-warranty** maintenance or support. Supplier should undertake to support the product for a minimum period of 5 years (post-warranty). Post Warranty, AMC charges for a period of 3 years (annual bases) should also be quoted separately in the financial bid.

24) Two sets of operational, service/troubleshooting manuals and diagrams to be supplied with "**SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL ".**

25) **The submission of tender** shall be deemed to be an admission on the part of the tenderer, had fully acquainted with the specifications, drawings etc. and no claim other than what stated in the tender shall be paid in the event of award of Purchase Order.

26) Expenditure involved towards any extra materials required for labour involved for successful installation of the equipment, if not quoted for, would have to be borne by the tenderer.

27) **Acceptance of this tender** form and submission of the quote within the stipulated time would be treated as:

a) The tenderer has understood all requirements as described in our Tender document.

b) Acceptance to provide/establish all the facilities mentioned in our tender without any price escalation, if the tenderer finds it necessary to add any hardware or software or any other materials during implementation.

c) Agreeing to execute order to the satisfaction of NCAOR or its authorized representatives within the stipulated time.

28) Training/installation charges should be clearly indicated including the scope of training.

29) Tender should clearly define the **infrastructure facilities required** for installation and commissioning of the equipment.

30) NCAOR will not be liable for any obligation until such time NCAOR has communicated to the successful bidder of its decision to release the Purchase Order.

31) **NCAOR will not be responsible for any postal delays.**

32) Bidders shall note that NCAOR will not entertain any correspondence or queries on the status of the offers received against this Tender Invitation.

33) Tenders from Manufacturers/Suppliers/Tenderers whose performance was not satisfactory in respect of quality of supplies and delivery schedules in any organizations, are liable for rejection. The tenders that do not comply with the above criteria and other terms & conditions are liable for rejection.

34) The Director, NCAOR does not bind to accept the lowest quotation and reserves the right to himself, to reject or partly accept any or all the quotations received without assigning any reason.

35) All disputes arising in connection with executing the purchase order will be subject to the Jurisdiction of the Courts in Goa only.

COMMERCIAL COMPLIANCE STATEMENT FOR SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL

Sr. No.	COMMERCIAL SPECIFICATION FOR SUPPLY OF UV-VIS MULTIPURPOSE SPECTROPHOTOMETER.	COMPLIED/ NOT COMPLIED	EXTRA FEATURES
1	A list of **reputed clients** to whom the firm has supplied similar items to be furnished along-with the quotation.		
2	In the TECHNICAL BID, the Bidder should furnish the Name and address of the Purchasers placed orders on similar equipment with order No, date, Description and quantity, Date of Supply alongwith Contact person Telephone No, Fax No, and e mail address of Purchaser.		
3	The Bidder should enclose copies of Purchase Orders only in the FINANCIAL BID.		
4	Quotation should be **valid for a period of 90 days** from the date of tender opening and the period of delivery required should also be clearly indicated.		
5	The **warranty period** and the kind of **post-warranty support** should be indicated. Warranty shall commence from the date of installation and acceptance of the complete equipment supplied under the Purchase Order / Contract.		
6	**Bidders** shall submit **EMD** along with their tender, **either By DD** drawn in favor of NCAOR, on any nationalized bank for a sum of ` 15,000/- (Rupees Fifteen Thousand only) payable at Vasco-da-Gama only **or in the form of a bank guarantee** for a sum of ` 15,000/-(Rupees Fifteen Thousand only) from any reputed bank (scheduled bank) initially valid for 180 days from the date of closing of the tender as per the proforma enclosed. This bank Guarantee in original shall be submitted along with the technical bid only.		
7	**Tender without EMD in the envelope containing technical bid shall be summarily rejected**. The EMD of unsuccessful bidders shall be returned within 30 days of the award of contract.		
8	Please **specify the Make/Brand** and Name of the Manufacturer with address, country of origin and currency in which rates are quoted.		
9	**The order acknowledgement** should be from the principals and if the Indian Agent is empowered to quote and to furnish order acknowledgement, a copy of agreement entered by you with the Indian Agent to be furnished.		
10	**Compliance Statement:** Equipments point-by-point comparison/compliance statement with **technical specification** indicated in the tender, should be enclosed along with your tender as well as any other extra features of the equipment be shown separately therein and also **compliance statement for all commercial terms** of the tender document.		
11	NCAOR is not entitled to issue form **"C/D"**. No Sales Tax or any other Tax shall be payable by us unless payment of the same is specifically mentioned by the suppliers in their bids and same is legally leviable.		
12	To avail duty concessions i.e. **Excise Duty** as per Govt. notification 10/97 & **Custom Duty** as per Govt. notification 51/96, NCAOR will provide exemption certificates. Hence, the rates should be split into basic cost and Excise Duty if any.		
13	**Technical Bid should contain** all details and specifications of the equipment offered, delivery schedule, warranty, payment term, installation, training, post-warranty, user-list, service support **WITHOUT PRICE** and **Financial bid should contain** details of the		

	price(s) of the item(s) quoted in the technical bid. The Technical bid should not contain any references to the pricing.		
14	**In case the technical bid contains any direct or indirect reference to quoted price the bid is liable to be rejected.**		
15	Submit your quote on F.O.R. destination basis. However tender should contain item-wise prices including total ex-works price, overall weight & dimensions of the equipment and cost of packing forwarding, approx. cost of freight charges for delivery up to Goa, India.		
16	A Committee constituted by the Director, NCAOR for the purpose reserves the right to open the bids. Only technical bids will be opened on the date and time mentioned in the tender document. The financial bids of those tenderers whose technical bids are found to be meeting our specifications only will be opened in their presence at date and time to be notified later.		
17	The firm to the full satisfaction of the NCAOR should carry out the **installation and commissioning** at the NCAOR premises and the time-frame for the whole process should be specified in the technical bid.		
18	A technical Committee constituted by the Director will assess the product supplied/installed for their quality and their conformity to the specifications provided by the firm in their quotations. Any item(s) identified by the Committee to be not as per the specifications or are found to be of inferior quality will be rejected, and the bills towards the supply will not be processed for payment till proper replacements are provided.		
19	**No advance payment** will be made. Payment shall be made after supply, installation and acceptance of the equipment by NCAOR.		
20	Suppliers should clearly define the mechanisms of **post-warranty** maintenance or support. Supplier should undertake to support the product for a minimum period of 5 years (post-warranty). Post Warranty, AMC charges for a period of 3 years (annual bases) should also be quoted separately in the financial bid.		
21	**Two sets of operational, service/troubleshooting manuals and diagrams to be supplied with "SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL"**		
22	**The submission of tender** shall be deemed to be an admission on the part of the tenderer, had fully acquainted with the specifications, drawings etc. and no claim other than what stated in the tender shall be paid in the event of award of Purchase Order.		
23	Expenditure involved towards any extra materials required for labour involved for successful installation of the equipment, if not quoted for, would have to be borne by the tenderer.		
24	**Acceptance of this tender** form and submission of the quote within the stipulated time would be treated as: • The tenderer has understood all requirements as described in our Tender document. • Acceptance to provide/establish all the facilities mentioned in our tender without any price escalation, if the tenderer finds it necessary to add any hardware or software or any other materials during implementation. • Agreeing to execute order to the satisfaction of NCAOR or its authorized representatives within the stipulated time.		
25	**Training /Installation charges** should be clearly indicated including the scope of training.		
26	Tender should clearly define the **infrastructure facilities required** for installation of the equipment.		

QUESTIONNAIRE

a. **Name of the Manufacturer / Tenderer**

b. **Full postal address with Telephone, Telefax, Email**

c. **Please specify whether Public Limited, Company, Private Organization or Partnership Firm**

d. **Nature of the Business**

e. **Date of Establishment**

f. **Present Turnover**

g. **Permanent Income Tax Ref. No.**

h. **C.S.T. / S.T. NO.**

i. **Address & Telephone Nos. Of your branch office in GOA (please specify whether Distributing/Servicing/Marketing the products)**

j. **Technical Compliance statement.**

k. **Commercial Compliance statement.**

l. **Reference of reputed Customers**

m. **Details of the highest order executed and value thereof**

n. **Authorization from Manufacturer/Supplier attached**

o. **Tender fee submitted/enclosed.**

p. **E.M.D. attached with BID.**

q. **Infrastructure facilities required for installation & commissioning attached**

r. **Technical Specifications/Literature/Brochure attached**

s. **Tender Acceptance**

TENDER ACCEPTANCE UNDERTAKING

To

The Director,
NCAOR, Headland Sada
Vasco - Goa

Having examined the tender document for **SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL**, we the undersigned, hereby offer to supply the equipment in conformity with all specifications and conditions set out in the tender document.

We enclosed all the relevant documents as per the tender.

We understand that you are not bound to accept the lowest or any tender received.

Date :

(Signature of Bidder)

Name :

Designation :

Seal

BANK GUARANTEE FORMAT FOR FURNISHING EMD

To

NATIONAL CENTRE FOR ANTARCTIC & OCEAN RESEARCH
Headland Sada, Vasco-da-Gama, GOA 403 804, INDIA

Whereas _____
(Hereinafter called the "tenderer"
has submitted their offer dated _____
for the supply of _____
(Herein after called the "tender"
WE_____ of having our registered office
At _____ are bound unto the NATIONAL
(Hereinafter called the Bank)
CENTRE FOR ANTARCTIC & OCEAN RESEARCH, Ministry of Earth Sciences, Govt. Of India having its office at Headland Sada, Vasco Goa 403 804, India (herein after called NCAOR which expression shall unless repugnant to the context or meaning thereof include all its successors, administrators, executors and assigns) in the sum of _____ for which payment will and truly to be made to. NCAOR, the Bank binds itself, its successors and assigns by these presents. Sealed with the common seal of the said Bank this _____day of _____2014.

THE CONDITIONS OF THIS OBLIGATION ARE:

1) If the tenderer withdraws or amends, impairs or derogates from the tender in any respect within the period of validity of this tender.

2) If the tenderer having been notified of the acceptance of his tender by NCAOR during the period of its validity.

2.a) If the tenderer fails to furnish the Performance security for the due performance of the contract.

2.b) Fails or refuses to execute the contract

We undertake to pay NCAOR up to the above amount upon receipt of its first written demand, without NCAOR having to substantiate its demand, provided that in its demand the NCAOR will note that the amount claimed by it is due to it owing to the occurrence of one or both the two conditions, specifying the occurred condition or conditions.

This guarantee is valid until the _____ day of _____2014.

Signature of the bank

NATIONAL CENTRE FOR ANTARCTIC & OCEAN RESEARCH
(*Ministry of Earth Sciences, Govt. Of India*)
Headland Sada, Vasco-da-Gama GOA 403 804, INDIA
Tel: 91- (0) 832 2525571 Telefax: 91- (0) 832 2525573
Email: warlu62@ncaor.gov.in Website: www.ncaor.gov.in

PUBLIC TENDER

Director, National Centre for Antarctic & Ocean Research (NCAOR) invites sealed tenders in two-parts (part I – Technical bid & part II Financial bid) super scribing Tender No. Item and due date from well established/ reputed manufacturers / authorized and bonafide vendors for supply of the following:-

Sl. No.	Tender No.	Item Description	Qty.	Cost of Tender Doc.	EMD
				``	``
1	NCAOR/PR-1199 /PT-35	**SUPPLY, INSTALLATION, TESTING AND COMMISSIONING OF NEXT GENERATION FIREWALL**	01 No.	500/-	15,000/-

Last date for issue of tender documents : **20.10.2014**
Last date for submission of quotation : **21.10.2014**
The details of tender documents are also available in our website http://www.ncaor.gov.in and Central Public Procurement Portal http://eprocure.gov.in. Interested suppliers may download the details and submit the quotation on or before the due date along with tender fee.
The quotation without tender fee will not be considered.
Tender forms can be obtained from the Procurement section of NCAOR on all working days either by post or in person between 1000 – 1600 hours on payment of tender fees in the form of crossed Demand Draft payable at Vasco-da-gama only, from a Nationalized bank drawn in favor of NCAOR along with separate requisition indicating tender number and item. Tender forms can be obtained by speed post by remitting ` 50/- by Indian bidders in addition to the cost of tender documents.
The Director, NCAOR is not responsible for any transitional/postal delays.
The quotations will be **opened on 22.10.2014** in the presence of tenderers or their authorized representatives.
The Director, NCAOR reserves the right to accept or reject any quotation in full or part thereof without assigning any reason.

Sd/-
For & on behalf of NCAOR