X810759 278 CH 278 90/80 29/10/2020 28/1

SPECIAL ADHESIVE Rs. 10000 PAKISTAN

SPECIAL ADHESIVE 29 OCT 2020 Rs. 10000 PAKISTAN

SPECIAL ADHESIVE Rs. 10000 PAKISTAN

SPECIAL ADHESIVE Rs. 10000 PAKISTAN

PAKISTAN 50 Rs SPECIAL ADHESIVE

روپیہ ۵۰

GHULAM SADIQ STAMP VENDOR
Lic # 79, Shop # 113, New Ruby Centre
Talpur Road, Boultan S.No.............. 33040
Market, Karachi. Date..............
Issue to with Address MR ...MUHAMMAD YAQOOB...
Through with AddressMR ....Advocate L.No.1459...
Purpose: ....
Value Rs: .... Attached: ....
Stamp Vendors Signature ....
(NOT USE FOR FREE WILL & DIVORCE PURPOSE)
Vendor Not Responsible for Fake Documents

01 SEP 2020

SPECIAL ADHESIVE Rs. 10000 PAKISTAN

SPECIAL ADHESIVE Rs. 10000 PAKISTAN

SPECIAL ADHESIVE Rs. 10000 PAKISTAN

KARACHI

29.10.2020

AGREEMENT

Provision of Core Network Upgradation on C&F Basis

THIS AGREMENT is executed at KARACHI, on this day September, 2020.

BETWEEN

M/s Institute of Business Administration, Karachi through its Registrar, located at **Main Campus, University Enclave, Karachi,** hereinafter called and referred to as "IBA" (which expression shall wherever the context so permits, be deemed to include its legal representatives, executors, successors and assigns) of the FIRST PART.

AND

M/s IBL Unisys (Pvt) Ltd, having its office at **# 2nd Floor, One IBL Center, Plot # 1, Block 7 & 8. DMMCHS, Tipu Sultan Enclave, Off Shahrah-e-Faisal, Karachi,** hereinafter referred to as "**SUPPLIER**" (which expression shall wherever the context so permits be deemed to include its legal representatives, executors, successor and assigns), through its Chief Financial Officer (Public Sector) **Mr. Rizwan Ahmed**, holding CNIC No. 42101-0901274-1 on the SECOND PART.

WHEREAS "IBA" intends to Provision of Core Network Upgradation vide tender # IT/12/19-20 for Provision of Core Network Upgradation (IBA requirement) discussions in respect of the same before the determination of scope will be held with "IBA" as "Provision of Core Network Upgradation" and "THE SUPPLIER" have offered the Provision of Core Network Upgradation (including but not limited to the "Provision of Core Network Upgradation" with complete accessories & peripherals proposed up to the satisfaction & handing over the material(s) to the "IBA" having accepted the offer in finished form complete in all respect.

IBL UNISYS (Pvt) Limited

NOW IT IS HEREBY AGREED & DECLARED BY AND BETWEEN THE PARTIES AS FOLLOWS:

WITNESSETH

"IBA" hereby offer to appoint "THE SUPPLIER" as their official for the specific purpose of "Provision of Core Network Upgradation" discussions in respect of the same with "IBA" before the determination of Scope of Provision of Core Network Upgradation with any/all other relevant details for presentation to "IBA" for Provision of Core Network Upgradation. "THE SUPPLIER" hereby agree to the offer of the "IBA" in acceptance of the terms & conditions here in below forth.

Article I
DUTIES & SCOPE OF SUPPLIES AND AGREEMENT

1.1 This Agreement includes, Provision of Core Network Upgradation, discussions with "IBA" before the determination of scope of supply with any/all other relevant details for presentation to "IBA". The description/BoQ is appended below:

S.No.	Technical specifications
1	**Core Switch – (Qty: 1)**
	The proposed core switch should include at least 48 x 1/10 SFP+ Ethernet L3 ports
	The proposed core switch should include at least 48 x 1G/10G RJ-45 copper Ethernet L3 ports
	The proposed core switch should include at least 24 x 40G QSFP+ ports
	The proposed core switch should have at least 1 x I/O slots available for future expansion.
	The core switch should have redundant control/supervisor cards with dedicated slots and should not use I/O slots.
	The proposed switch should have redundant AC power supplies (N+1).
	The switch should have redundant switch fabrics with stateful switchover.
	Should support major layer 3 protocols like OSPF, BGP, IS-IS etc. Any license required should be part of the proposal.
	The Core switch shall support switching fabric capacity of minimum 15 Tbps & forwarding rate of more than 7 bpps or higher.
	Proposed switch should support line rate processing for all the interfaces.
	The core switches should support minimum 3 Tbps per slot
	The core switch should support SDN architecture with option to configure the components from centralized SDN controller if required in future.
	Must support advanced dynamic Routing Protocol and advanced QoS features
	There should not be any head of line blocking architecture to avoid any packet loss.
	Should support industry standards like VXLAN and be able to terminate VXLAN for VLAN interoperability. Any license required for VXLAN should be part of the solution.
	The proposed switch must support ISSU (In Service Software Upgrade)
	The proposed switch should provide Non Stop Forwarding during supervisor switchover
	The switch should have redundant fan trays and the fan trays should be hot swappable
	Online insertion and removal (OIR) of all redundant components: Supervisor, fabric, power supply, and fan trays etc.
	Should support features like SPAN and Ethanalyzers
	Proposed hardware should support configuration management like "roll back" and Role Based Access Control

OFFICE SUPERINTENDENT
Stamp Office, City Court
Karachi
29.10.2020
29 OCT 2020

UNIS (Pvt) Limited

	Should support standard Security features and protocols like Authentication, authorization, and accounting (AAA), Secure Shell (SSH) Protocol Version 2, Simple Network Management Protocol Version 3 (SNMPv3) support, Port Security and IEEE 802.1x authentication and RADIUS
2	**(Server Farm Switch) – (Qty: 2)**
	The proposed switch should have 48 x 1G/10G Base T RJ 45 Ports.
	The switch should also have at least 4 x 40G QSFP28 Ports
	All ports must be line-rate non-blocking
	Should include Layer 3 features, including full OSPF, VXLAN, and BGP. Any license required should be part of the proposal
	The switch should support below standards
	IEEE 802.1Q: VLAN Tagging
	IEEE 802.1s: Multiple VLAN Instances of Spanning Tree Protocol
	IEEE 802.1D: Spanning Tree Protocol
	IEEE 802.1p: CoS Prioritization
	IEEE 802.3ad: Link Aggregation Control Protocol (LACP)
	IEEE 802.1w: Rapid Reconfiguration of Spanning Tree Protocol
	IEEE 802.1ab: LLDP
	Should have dual redundant power supplies
	Should have redundant hot swappable fans
	Value Added Services: - (a) Bidder should provide 5 Days training on proposed solution for three ICT persons in Regional Authorized Training centre. (b) The successful bidder should arrange executive briefing sessions, encompassing all features and technical aspects, for ICT senior management on New technology trends, smart classrooms, IOT & SDN's at regional headquarter of the principal / manufacturer from their marketing budget.
3	**PoE Access Switch (Qty: 20)**
	The switch should have 48 x 1G PoE+ ports
	The switch should have 4 x 10G SFP uplink ports
	The switch should support more than 170Gbps switching capacity and at least 130 Mpps of forwarding rate
	The switch should be stackable and should support at least 6 switches in a stack
	The switch should support redundant power supply
	Support for full layer 3 routing functionality (RIP, OSPF, Static, PBR)
	Should support IEEE MacSec encryption
	Support for NetFlow/Sflow or equivalent
	The switch should provide features such as Layer 2, Routed Access (RIP, OSPF), PBR, PIM Stub Multicast, PVLAN, QoS, 802.1X. Any license required should be part of the proposal
	Fully managed switch
	RADIUS and TACACS authentication
	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
	Support at least 512 or higher ACL rules
	SNMPv3
4	**Internet Router – (Qty: 2)**
	The proposed router should not be more 1 RU form factor since we have limited space available in the racks
	Should have at least 2 x RJ45 GE + 2 x SFP WAN ports
	Dual AC power supplies required
	Proposed router should have at least 2 interface module Slots.
	Proposed router must support a throughput of at least 2 Gbps or higher.
	The router should support security features such as Firewall, VPN, ACL, IPSEC VPN etc.

	The Router should support encrypted throughput of at least 500 Mbps
	Proposed routers should have multi core processors for high speed WAN Connections
	The proposed router should support advanced networking protocols such as L2TPv3, BFD, MPLS, VRF, VXLAN etc.
	Proposed router should support features like SD-WAN and should be able to support SD-WAN by simply changing the software
	Should support Layer 3 routing protocols including RIP, OSPF, IS-IS, BGP, PBR etc.
	The router must support Overlay features like
	L2TPv3
	GRE
	MPLS
	Should support Online Insertion and Removal of interface modules
	Proposed hardware should support QoS features like
	CBWFQ
	Performance Routing
	WRED etc
	Telnet
	Simple Network Management Protocol Version 3 (SNMPv3)
	Secure Shell (SSH)
	RADIUS and TACACS+
5	**Internet Firewall (Qty: 2)**
	The firewall should be Next Generation Firewall
	The proposed brand must be either in Challenger or Leader MQ of latest Gartner NGFW MQ
	Required either 8 x RJ 45 GE + 4 x SFP 1G Ethernet ports or 8 x GE Combo Ethernet ports
	Required NGFW + NGIPS throughput more than 2 Gbps (1024B Packet) with all features enabled
	Required maximum concurrent sessions at least 400,000 with Application Visibility and Control enabled
	Should support more than 21,500 new connections per second with Application Visibility and Control enabled
	More than 1 Gbps of IPSEC VPN throughput
	Should support local as well as centralized management
	AC power supply
	The proposed firewalls solution shall be capable of detecting link failure in addition to device failure
	The proposed firewalls shall support standards based link aggregation (IEEE 802.3ad) to achieve higher bandwidth
	NGIPS with full contextual awareness of users, infrastructure, applications, and content to detect multi-vector threats
	Required granular Application Visibility and Control with support for more than 4,000 applications.
	Required URL Filtering with support for more than 120 Million URLs categorized and more than 80 URLs categories.
	Detection of Geo location of IP Addresses
	The firewall should support SSL decryption to enforce NGIPS & NGIPS policies
	The firewall should support SSL decryption of the published web servers using the certificate server of the servers and applying the layer 7 policies
	The firewall should support rate-limiting traffic on the basis of users, applications etc.
	Identify and control applications on any port, not just standard ports (including applications using HTTP or other protocols)

	Provide application function control
	Identify and control applications sharing the same connection
	Fine-grained visibility and policy control over application access / functionality
	Integrate with Microsoft Active Directory Server for implementing user based application access control
	Support creation of security policy based on AD Users and Groups in addition to source/destination IP
	Support AAA, RADIUS, SNMP
	Support detection and prevention against tunnel /encapsulated /encrypted attacks, p2p application related threats
	Protect against IP and TCP fragmentation related attacks
	Support creation of user-defined application protocol detectors
	File control - detect and block users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols.
	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.
	Protocols: FTP, HTTP, SMTP, IMAP, and POP3
	Direction: Upload, Download, Both
	File Types: Office Documents, Archive, Multimedia, Executable, PDF etc.
	Automated threat feed and IPS signature updates
	Automated threat correlation
	Support policy control by port and protocol, application, user/group, IP address, IPV6 rules/objects and multicast rules/objects etc.
	Allow administrators to create custom IPS signatures
	When an IPS signature is matched, the following configurable actions can be automatically taken:
	Detailed attack logging with hyperlink to IPS encyclopedia references
	SNMP traps
	Packet logging for forensic studies
	Pass, block or reset TCP sessions
	Analyzes files at point of entry to catch malwares, block malwares in real-time using one-to-one signature matching or machine learning/AI etc.
	Support network traffic classification application identification across all ports
	Provide multiple mechanisms for classifying applications and application identification technology based upon Intrusion Prevention System (IPS) or deep packet inspection.
	Provide the ability to allow the organization to create customized application rules
	Have searchable list of currently identified applications
	Accurately classify traffic based on application (example: Gmail or Facebook etc.)
	Be able to create filters to control groups of application based on category, sub category, technology, risk or characteristics etc.
	Support user-identification allowing AD, LDAP, RADIUS groups, or users to access a particular application, while denying others
	Web based on-box Management/GUI administration
	Proposed Firewalls solution must be centrally managed from Web-Based Graphical User Interface (GUI)
	SNMP,SYSLOG and Netflow or equivalent
	The proposed firewalls shall have a reporting management system capable of generating reports on a manual ad-hoc or schedule (daily, weekly, monthly, etc) basis.

	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as trouble-ticketing systems, Security Information and Event Managers (SIEMs), systems management platforms, and log management tools.
	The solution should be able to send alert messages at least through Console Alerting or Email mechanism
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to export SNMP information to network management systems.
	Three Years Subscription required for all required features (NGW, NGIPS, Advance Malware Protection, and ULR Filtering)
6	**DC Firewall (Qty: 2)**
	The firewall should be Next Generation Firewall
	The proposed brand must be either in Challenger or Leader MQ of latest Gartner NGFW MQ
	Required either 8 x RJ 45 GE + 4 x SFP 1G Ethernet ports or 8 x GE Combo Ethernet ports
	Required NGFW + NGIPS throughput at least 1.5 Gbps (1024B Packet) with all features enabled
	Required maximum concurrent sessions at least 200,000 with Application Visibility and Control enabled
	Should support at least 15,000 new connections per second with Application Visibility and Control enabled
	At least 2 Gbps of IPSEC VPN throughput
	Support at least 500 SSL VPN sessions.
	License for 100 SSL VPN must be included in the proposal.
	Should support local as well as centralized management
	AC power supply
	The proposed firewalls solution shall be capable of detecting link failure in addition to device failure
	The proposed firewalls shall support standards based link aggregation (IEEE 802.3ad) to achieve higher bandwidth
	NGIPS with full contextual awareness of users, infrastructure, applications, and content to detect multi-vector threats
	Required granular Application Visibility and Control with support for more than 4,000 applications.
	Required URL Filtering with support for more than 120 Million URLs categorized and more than 80 URLs categories.
	Detection of Geo location of IP Addresses
	The firewall should support SSL decryption to enforce NGIPS & NGIPS policies
	The firewall should support SSL decryption of the published web servers using the certificate server of the servers and applying the layer 7 policies
	The firewall should support rate-limiting traffic on the basis of users, applications etc.
	Identify and control applications on any port, not just standard ports (including applications using HTTP or other protocols)
	Provide application function control
	Identify and control applications sharing the same connection
	Fine-grained visibility and policy control over application access / functionality
	Integrate with Microsoft Active Directory Server for implementing user based application access control

GOVT OF SINDH
KARACHI-PAKISTAN

	Support creation of security policy based on AD Users and Groups in addition to source/destination IP
	Support AAA, RADIUS, SNMP
	Support detection and prevention against tunnel /encapsulated /encrypted attacks, p2p application related threats
	Protect against IP and TCP fragmentation related attacks
	Support creation of user-defined application protocol detectors
	File control - detect and block users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols.
	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.
	Protocols: FTP, HTTP, SMTP, IMAP, and POP3
	Direction: Upload, Download, Both
	File Types: Office Documents, Archive, Multimedia, Executable, PDF etc.
	Automated threat feed and IPS signature updates
	Automated threat correlation
	Support policy control by port and protocol, application, user/group, IP address, IPV6 rules/objects and multicast rules/objects etc.
	Allow administrators to create custom IPS signatures
	When an IPS signature is matched, the following configurable actions can be automatically taken:
	Detailed attack logging with hyperlink to IPS encyclopedia references
	SNMP traps
	Packet logging for forensic studies
	Pass, block or reset TCP sessions
	Analyzes files at point of entry to catch malwares, block malwares in real-time using one-to-one signature matching or machine learning/AI etc.
	Support network traffic classification application identification across all ports
	Provide multiple mechanisms for classifying applications and application identification technology based upon Intrusion Prevention System (IPS) or deep packet inspection.
	Provide the ability to allow the organization to create customized application rules
	Have searchable list of currently identified applications
	Accurately classify traffic based on application (example: Gmail or Facebook etc.)
	Be able to create filters to control groups of application based on category, sub category, technology, risk or characteristics etc.
	Support user-identification allowing AD, LDAP, RADIUS groups, or users to access a particular application, while denying others
	Web based on-box Management/GUI administration
	Proposed Firewalls solution must be centrally managed from Web-Based Graphical User Interface (GUI)
	SNMP,SYSLOG and Netflow or equivalent
	The proposed firewalls shall have a reporting management system capable of generating reports on a manual ad-hoc or schedule (daily, weekly, monthly, etc) basis.
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as trouble-ticketing systems, Security Information and Event Managers (SIEMs), systems management platforms, and log management tools.

	The solution should be able to send alert messages at least through Console Alerting or Email mechanism
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to export SNMP information to network management systems.
7	**Centralized Management, Monitoring & Reporting: (Qty: 1)**
	Appliance based Centralized security management console and database repository for event and policy management of NGFW, NGIPS, and Advance Malware Detection and Prevention
	Centralized configuration, logging, monitoring, and reporting for NGFW, NGIPS and Advance Malware Detection and Prevention
	Required Centralized Management for Minimum 10 NGFW Appliances
	Automatically aggregate and correlate information generated by Next Generation Firewall, Next Generation and Advance Malware Detection
	Provide full stack visibility including
	Threats
	Users
	Web Applications
	Client applications
	Application protocols:
	File transfers
	Malware
	CNC servers
	Network servers
	Server/host operating system
	Mobile devices
	Virtual machines
	Role-based device user management
	Customizable dashboard with custom and/or template-based reports
	Correlation and remediation features for real-time threat response
	Network behavior and performance monitoring
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as trouble-ticketing systems, Security Information and Event Managers (SIEMs), systems management platforms, and log management tools.
8	**Voice Gateway Router : (QTY:2)**
	The proposed router should not be more 1 RU form factor since limited space is available in the racks
	Should have at least 2 x RJ45 GE + 2 x SFP WAN ports
	Proposed router should have at least 3 interface module Slots.
	At least 2 of the interface slots should be empty for future expansion
	Proposed router must support a throughput of at least 100 Mbps or higher.
	The proposed router should support upgradation to at least 2 Gbps throughput by simply adding a license without any hardware addition.
	The proposed router should include at least 4 x FXO interfaces
	Proposed router provide voice gateway functionality and any license required should be part of the proposal
	Should support at least 400 SIP/H.323 Sessions and any license required should be part of the proposal
	Router should provide SIP trunk and should include licenses for at least 70 simultaneous SIP Sessions.
	Should include at least 64 channel DSP module for handling voice traffic
	Should support features to act as Call Control for IP Phones supporting at least 100 IP Phones

	Should support at least 12 x E1/PRI Interfaces to support digital voice interconnections
	The router should support security features such as Firewall, VPN, ACL, DNS Security, IPSEC, SSLVPN etc.
	The Router Should support encrypted throughput of at least 500 Mbps
	Proposed routers should have multi core processors for high speed WAN Connections
	Should support Service Level Agreements (SLAs) for the monitoring of the WAN links
	The proposed router should support advanced networking protocols such as L2TPv3, BFD, MPLS, VRF, VXLAN etc.
	The routers should support features like Application Optimization to enhance end user experience by having some sort of caching etc. in case of low bandwidth WAN Links.
	Should support WAN optimization features as below:
	TCP Flow Optimization
	Persistent LZ Compression
	DRE Compression
	Application Optimizations for file sharing, emails, web apps, enterprise apps etc.
	Proposed router should support features like SD-WAN and should be able to support SD-WAN by simply changing the software
	Should support SDN.
	Should support Next Generation Encryption features as below.
	AES-128-GCM for Authenticated Encryption
	HMAC-SHA256 for Authentication
	ECDSA-P256 for Digital Signatures
	SHA-256 for Hashing
	ECDH-P256 for Key Establishment.
	Should support Layer 3 routing protocols including RIP, OSPF, IS-IS, BGP, PBR etc.
	The router must support Over lay features like
	L2TPv3
	GRE
	MPLS
	Should have at least 4GB DRAM, with option to upgrade to 16GB.
	Should have at least and 4GB Flash, with option to upgrade up to 16GB.
	Should support Online Insertion and Removal of interface modules
	Proposed hardware should support QoS features like:
	CBWFQ
	Performance Routing
	WRED etc
	Proposed router must comply with following standards
	TIA-968-B
	CS-03
	ANSI T1.101
	ITU-T G.823, G.824
	IEEE 802.3

1.2 THE SUPPLIER" agrees to provide Supply of Provision of Core Network Upgradation with complete & all accessories to "IBA" whenever and wherever required as per the terms & conditions of this Agreement.

1.3 "THE SUPPLIER" will coordinate with Head of Procurement, of the "IBA" who will assist "THE SUPPLIER" in supervision of proposed Provision of Core Network Upgradation.

1.4 “THE SUPPLIER” hereby agrees to accept variation, if occurred, in scope of supply with mutual consent on approved cost/price/charges/amount inclusive of all taxes and levies.

1.5 “THE SUPPLIER” will visit the Purchase Offices located at Main Campus, University Enclave, Karachi as & when required with prior appointment.

1.6 All equipment mentioned in Purchase Order will be delivered new, in packed condition directly to the location, as per the discretion of IBA. If equipment delivered is not conforming to the specifications and Bill of Quantity, the equipment will not be accepted.

1.7 All Equipment shall be individually packed in standard packing provided by the manufacturer for onwards transportation and delivery. Any item damaged during transportation will be replaced by the bidders at their own cost.

1.8 The Supplier will provide Assurance on a Rs.100/- valued stamp paper that the item Provision of Core Network Upgradation in required quantity is not smuggled from any country(ies) / source(s) and not refurbished / reconditioned remolded etc.

1.9 The country for this procurement is Pakistan. M/s IBL Unisys (Pvt) Ltd supply any commodities or services that are manufactured or assembled in, shipped from, transported through, or otherwise involving any of the country i.e., INDIA & ISRAEL.

1.10Shipping will be made by the supplier preferably through the National Vessel/Airline. Shipment by INDIA nor ISRAELI Vessel/Airline is not allowed.

1.11The partial shipment of stores shall not be allowed; the complete stores will be shipped as one consignment.

1.12Head of Procurement in coordination of technical department will inspect the items as per specifications after arrival at Stores and will carry out necessary testing of equipment and render a ***Certificate of Correctness.***

1.13Material of this order is subject to final inspection from Competent Authority Technical Team at the time of delivery.

1.14Configuration, installation and implementation will be the responsibility of the Partner; however ICT Operation Team will be available to make the process rational.

1.15Partner would be responsible to provide three years warranty backed by principal, Support should include 24x7 Support direct from principal except for Access Layer Switches applied 8x5xNBD replacement support facility is acceptable.

1.16Mission Critical Direct 24x7x4 onsite engineering support for Core Switch, Server form switch, Internet Router, Internet Firewall, DC Firewall and Voice gateway router.

1.17NBD Support for access layer switch.

1.18Transportation and labor inclusive.

1.19Warranty should be fully backed by principal / manufacturer. Bidder must submit appropriate service agreement details / approval to guarantee required service level

Article II
REMUNERATION

2.1 The bid price offered by the Supplier is US$ 165,157.00. on C&F basis includes Cost & Freight of Goods, Insurance Charges, Charges for Custom Clearance at Karachi

IBL UNISYS (Pvt) Limited

Port & Sellers LC Charges for Provision of Core Network Upgradation vide tender # IT/12/19-20. The cost is inclusive of labor/transportation / supplies / etc.

S. No	Make and Model	C&F Bid Value (Foreign Currency)	Qty	Total Bid Value
1	Core Switch	$40,398.76	1	$40,399
2	Server Farm Switch	$6,746.37	2	$13,493
3	POE Access Switch	$2,554.63	20	$51,093
4	Internet Router	$1,322.10	2	$2,644
5	Internet Firewall	$4,406.32	2	$8,813
6	DC Firewall	$2,012.29	2	$4,025
7	Centralized Management, Monitoring & Reporting	$15,921.08	1	$15,921
8	Voice Gateway Routers	$14,385.25	2	$28,771
Total				$165,157

Annex-A

Technical specifications

S. No.	Technical specifications
1	**Core Switch – (Qty: 1)**
	The proposed core switch should include at least 48 x 1/10 SFP+ Ethernet L3 ports
	The proposed core switch should include at least 48 x 1G/10G RJ-45 copper Ethernet L3 ports
	The proposed core switch should include at least 24 x 40G QSFP+ ports
	The proposed core switch should have at least 1 x I/O slots available for future expansion.
	The core switch should have redundant control/supervisor cards with dedicated slots and should not use I/O slots.
	The proposed switch should have redundant AC power supplies (N+1).
	The switch should have redundant switch fabrics with stateful switchover.
	Should support major layer 3 protocols like OSPF, BGP, IS-IS etc. Any license required should be part of the proposal.
	The Core switch shall support switching fabric capacity of minimum 15 Tbps & forwarding rate of more than 7 bpps or higher.
	Proposed switch should support line rate processing for all the interfaces.
	The core switches should support minimum 3 Tbps per slot
	The core switch should support SDN architecture with option to configure the components from centralized SDN controller if required in future.
	Must support advanced dynamic Routing Protocol and advanced QoS features
	There should not be any head of line blocking architecture to avoid any packet loss.
	Should support industry standards like VXLAN and be able to terminate VXLAN for VLAN interoperability. Any license required for VXLAN should be part of the solution.
	The proposed switch must support ISSU (In Service Software Upgrade)
	The proposed switch should provide Non Stop Forwarding during supervisor switchover
	The switch should have redundant fan trays and the fan trays should be hot swappable
	Online insertion and removal (OIR) of all redundant components: Supervisor, fabric, power supply, and fan trays etc.
	Should support features like SPAN and Ethanalyzers
	Proposed hardware should support configuration management like “roll back” and Role Based Access Control
	Should support standard Security features and protocols like Authentication, authorization, and accounting (AAA), Secure Shell (SSH) Protocol Version 2, Simple Network Management Protocol Version 3 (SNMPv3) support, Port Security and IEEE 802.1x authentication and RADIUS
2	**(Server Farm Switch) – (Qty: 2)**
	The proposed switch should have 48 x 1G/10G Base T RJ 45 Ports.

	The switch should also have at least 4 x 40G QSFP28 Ports
	All ports must be line-rate non-blocking
	Should include Layer 3 features, including full OSPF, VXLAN, and BGP. Any license required should be part of the proposal
	The switch should support below standards
	IEEE 802.1Q: VLAN Tagging
	IEEE 802.1s: Multiple VLAN Instances of Spanning Tree Protocol
	IEEE 802.1D: Spanning Tree Protocol
	IEEE 802.1p: CoS Prioritization
	IEEE 802.3ad: Link Aggregation Control Protocol (LACP)
	IEEE 802.1w: Rapid Reconfiguration of Spanning Tree Protocol
	IEEE 802.1ab: LLDP
	Should have dual redundant power supplies
	Should have redundant hot swappable fans
	Value Added Services: - (a) Bidder should provide 5 Days training on proposed solution for three ICT persons in Regional Authorized Training centre. (b) The successful bidder should arrange executive briefing sessions, encompassing all features and technical aspects, for ICT senior management on New technology trends, smart classrooms, IOT & SDN's at regional headquarter of the principal / manufacturer from their marketing budget.
3	**PoE Access Switch (Qty: 20)**
	The switch should have 48 x 1G PoE+ ports
	The switch should have 4 x 10G SFP uplink ports
	The switch should support more than 170Gbps switching capacity and at least 130 Mpps of forwarding rate
	The switch should be stackable and should support at least 6 switches in a stack
	The switch should support redundant power supply
	Support for full layer 3 routing functionality (RIP, OSPF, Static, PBR)
	Should support IEEE MacSec encryption
	Support for NetFlow/Sflow or equivalent
	The switch should provide features such as Layer 2, Routed Access (RIP, OSPF), PBR, PIM Stub Multicast, PVLAN, QoS, 802.1X. Any license required should be part of the proposal
	Fully managed switch
	RADIUS and TACACS authentication
	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
	Support at least 512 or higher ACL rules
	SNMPv3
4	**Internet Router – (Qty: 2)**
	The proposed router should not be more 1 RU form factor since we have limited space available in the racks
	Should have at least 2 x RJ45 GE + 2 x SFP WAN ports
	Dual AC power supplies required
	Proposed router should have at least 2 interface module Slots.
	Proposed router must support a throughput of at least 2 Gbps or higher.
	The router should support security features such as Firewall, VPN, ACL, IPSEC VPN etc.
	The Router should support encrypted throughput of at least 500 Mbps
	Proposed routers should have multi core processors for high speed WAN Connections
	The proposed router should support advanced networking protocols such as L2TPv3, BFD, MPLS, VRF, VXLAN etc.
	Proposed router should support features like SD-WAN and should be able to support SD-WAN by simply changing the software
	Should support Layer 3 routing protocols including RIP, OSPF, IS-IS, BGP, PBR etc.
	The router must support Overlay features like
	L2TPv3
	GRE
	MPLS

UNISYS (Pvt) Limited

	Should support Online Insertion and Removal of interface modules
	Proposed hardware should support QoS features like
	CBWFQ
	Performance Routing
	WRED etc
	Telnet
	Simple Network Management Protocol Version 3 (SNMPv3)
	Secure Shell (SSH)
	RADIUS and TACACS+
5	**Internet Firewall (Qty: 2)**
	The firewall should be Next Generation Firewall
	The proposed brand must be either in Challenger or Leader MQ of latest Gartner NGFW MQ
	Required either 8 x RJ 45 GE + 4 x SFP 1G Ethernet ports or 8 x GE Combo Ethernet ports
	Required NGFW + NGIPS throughput more than 2 Gbps (1024B Packet) with all features enabled
	Required maximum concurrent sessions at least 400,000 with Application Visibility and Control enabled
	Should support more than 21,500 new connections per second with Application Visibility and Control enabled
	More than 1 Gbps of IPSEC VPN throughput
	Should support local as well as centralized management
	AC power supply
	The proposed firewalls solution shall be capable of detecting link failure in addition to device failure
	The proposed firewalls shall support standards based link aggregation (IEEE 802.3ad) to achieve higher bandwidth
	NGIPS with full contextual awareness of users, infrastructure, applications, and content to detect multi-vector threats
	Required granular Application Visibility and Control with support for more than 4,000 applications.
	Required URL Filtering with support for more than 120 Million URLs categorized and more than 80 URLs categories.
	Detection of Geo location of IP Addresses
	The firewall should support SSL decryption to enforce NGIPS & NGIPS policies
	The firewall should support SSL decryption of the published web servers using the certificate server of the servers and applying the layer 7 policies
	The firewall should support rate-limiting traffic on the basis of users, applications etc.
	Identify and control applications on any port, not just standard ports (including applications using HTTP or other protocols)
	Provide application function control
	Identify and control applications sharing the same connection
	Fine-grained visibility and policy control over application access / functionality
	Integrate with Microsoft Active Directory Server for implementing user based application access control
	Support creation of security policy based on AD Users and Groups in addition to source/destination IP
	Support AAA, RADIUS, SNMP
	Support detection and prevention against tunnel /encapsulated /encrypted attacks, p2p application related threats
	Protect against IP and TCP fragmentation related attacks
	Support creation of user-defined application protocol detectors
	File control - detect and block users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols.
	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.
	Protocols: FTP, HTTP, SMTP, IMAP, and POP3
	Direction: Upload, Download, Both
	File Types: Office Documents, Archive, Multimedia, Executable, PDF etc.

	Automated threat feed and IPS signature updates
	Automated threat correlation
	Support policy control by port and protocol, application, user/group, IP address, IPV6 rules/objects and multicast rules/objects etc.
	Allow administrators to create custom IPS signatures
	When an IPS signature is matched, the following configurable actions can be automatically taken:
	Detailed attack logging with hyperlink to IPS encyclopedia references
	SNMP traps
	Packet logging for forensic studies
	Pass, block or reset TCP sessions
	Analyzes files at point of entry to catch malwares, block malwares in real-time using one-to-one signature matching or machine learning/AI etc.
	Support network traffic classification application identification across all ports
	Provide multiple mechanisms for classifying applications and application identification technology based upon Intrusion Prevention System (IPS) or deep packet inspection.
	Provide the ability to allow the organization to create customized application rules
	Have searchable list of currently identified applications
	Accurately classify traffic based on application (example: Gmail or Facebook etc.)
	Be able to create filters to control groups of application based on category, sub category, technology, risk or characteristics etc.
	Support user-identification allowing AD, LDAP, RADIUS groups, or users to access a particular application, while denying others
	Web based on-box Management/GUI administration
	Proposed Firewalls solution must be centrally managed from Web-Based Graphical User Interface (GUI)
	SNMP,SYSLOG and Netflow or equivalent
	The proposed firewalls shall have a reporting management system capable of generating reports on a manual ad-hoc or schedule (daily, weekly, monthly, etc) basis.
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as trouble-ticketing systems, Security Information and Event Managers (SIEMs), systems management platforms, and log management tools.
	The solution should be able to send alert messages at least through Console Alerting or Email mechanism
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to export SNMP information to network management systems.
	Three Years Subscription required for all required features (NGW, NGIPS, Advance Malware Protection, and ULR Filtering)
6	**DC Firewall (Qty: 2)**
	The firewall should be Next Generation Firewall
	The proposed brand must be either in Challenger or Leader MQ of latest Gartner NGFW MQ
	Required either 8 x RJ 45 GE + 4 x SFP 1G Ethernet ports or 8 x GE Combo Ethernet ports
	Required NGFW + NGIPS throughput at least 1.5 Gbps (1024B Packet) with all features enabled
	Required maximum concurrent sessions at least 200,000 with Application Visibility and Control enabled
	Should support at least 15,000 new connections per second with Application Visibility and Control enabled
	At least 2 Gbps of IPSEC VPN throughput
	Support at least 500 SSL VPN sessions.
	License for 100 SSL VPN must be included in the proposal.
	Should support local as well as centralized management
	AC power supply

	The proposed firewalls solution shall be capable of detecting link failure in addition to device failure
	The proposed firewalls shall support standards based link aggregation (IEEE 802.3ad) to achieve higher bandwidth
	NGIPS with full contextual awareness of users, infrastructure, applications, and content to detect multi-vector threats
	Required granular Application Visibility and Control with support for more than 4,000 applications.
	Required URL Filtering with support for more than 120 Million URLs categorized and more than 80 URLs categories.
	Detection of Geo location of IP Addresses
	The firewall should support SSL decryption to enforce NGIPS & NGIPS policies
	The firewall should support SSL decryption of the published web servers using the certificate server of the servers and applying the layer 7 policies
	The firewall should support rate-limiting traffic on the basis of users, applications etc.
	Identify and control applications on any port, not just standard ports (including applications using HTTP or other protocols)
	Provide application function control
	Identify and control applications sharing the same connection
	Fine-grained visibility and policy control over application access / functionality
	Integrate with Microsoft Active Directory Server for implementing user based application access control
	Support creation of security policy based on AD Users and Groups in addition to source/destination IP
	Support AAA, RADIUS, SNMP
	Support detection and prevention against tunnel /encapsulated /encrypted attacks, p2p application related threats
	Protect against IP and TCP fragmentation related attacks
	Support creation of user-defined application protocol detectors
	File control - detect and block users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols.
	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.
	Protocols: FTP, HTTP, SMTP, IMAP, and POP3
	Direction: Upload, Download, Both
	File Types: Office Documents, Archive, Multimedia, Executable, PDF etc.
	Automated threat feed and IPS signature updates
	Automated threat correlation
	Support policy control by port and protocol, application, user/group, IP address, IPV6 rules/objects and multicast rules/objects etc.
	Allow administrators to create custom IPS signatures
	When an IPS signature is matched, the following configurable actions can be automatically taken:
	Detailed attack logging with hyperlink to IPS encyclopedia references
	SNMP traps
	Packet logging for forensic studies
	Pass, block or reset TCP sessions
	Analyzes files at point of entry to catch malwares, block malwares in real-time using one-to-one signature matching or machine learning/AI etc.
	Support network traffic classification application identification across all ports
	Provide multiple mechanisms for classifying applications and application identification technology based upon Intrusion Prevention System (IPS) or deep packet inspection.
	Provide the ability to allow the organization to create customized application rules
	Have searchable list of currently identified applications
	Accurately classify traffic based on application (example: Gmail or Facebook etc.)
	Be able to create filters to control groups of application based on category, sub category, technology, risk or characteristics etc.

	Support user-identification allowing AD, LDAP, RADIUS groups, or users to access a particular application, while denying others
	Web based on-box Management/GUI administration
	Proposed Firewalls solution must be centrally managed from Web-Based Graphical User Interface (GUI)
	SNMP,SYSLOG and Netflow or equivalent
	The proposed firewalls shall have a reporting management system capable of generating reports on a manual ad-hoc or schedule (daily, weekly, monthly, etc) basis.
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as trouble-ticketing systems, Security Information and Event Managers (SIEMs), systems management platforms, and log management tools.
	The solution should be able to send alert messages at least through Console Alerting or Email mechanism
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to export SNMP information to network management systems.
7	**Centralized Management, Monitoring & Reporting: (Qty: 1)**
	Appliance based Centralized security management console and database repository for event and policy management of NGFW, NGIPS, and Advance Malware Detection and Prevention
	Centralized configuration, logging, monitoring, and reporting for NGFW, NGIPS and Advance Malware Detection and Prevention
	Required Centralized Management for Minimum 10 NGFW Appliances
	Automatically aggregate and correlate information generated by Next Generation Firewall, Next Generation and Advance Malware Detection
	Provide full stack visibility including
	Threats
	Users
	Web Applications
	Client applications
	Application protocols:
	File transfers
	Malware
	CNC servers
	Network servers
	Server/host operating system
	Mobile devices
	Virtual machines
	Role-based device user management
	Customizable dashboard with custom and/or template-based reports
	Correlation and remediation features for real-time threat response
	Network behavior and performance monitoring
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as trouble-ticketing systems, Security Information and Event Managers (SIEMs), systems management platforms, and log management tools.
8	**Voice Gateway Router : (QTY:2)**
	The proposed router should not be more 1 RU form factor since limited space is available in the racks
	Should have at least 2 x RJ45 GE + 2 x SFP WAN ports
	Proposed router should have at least 3 Interface module Slots.
	At least 2 of the interface slots should be empty for future expansion
	Proposed router must support a throughput of at least 100 Mbps or higher.
	The proposed router should support upgradation to at least 2 Gbps throughput by simply adding a license without any hardware addition.
	The proposed router should include at least 4 x FXO interfaces

	Proposed router provide voice gateway functionality and any license required should be part of the proposal
	Should support at least 400 SIP/H.323 Sessions and any license required should be part of the proposal
	Router should provide SIP trunk and should include licenses for at least 70 simultaneous SIP Sessions.
	Should include at least 64 channel DSP module for handling voice traffic
	Should support features to act as Call Control for IP Phones supporting at least 100 IP Phones
	Should support at least 12 x E1/PRI Interfaces to support digital voice interconnections
	The router should support security features such as Firewall, VPN, ACL, DNS Security, IPSEC, SSLVPN etc.
	The Router Should support encrypted throughput of at least 500 Mbps
	Proposed routers should have multi core processors for high speed WAN Connections
	Should support Service Level Agreements (SLAs) for the monitoring of the WAN links
	The proposed router should support advanced networking protocols such as L2TPv3, BFD, MPLS, VRF, VXLAN etc.
	The routers should support features like Application Optimization to enhance end user experience by having some sort of caching etc. in case of low bandwidth WAN Links.
	Should support WAN optimization features as below:
	TCP Flow Optimization
	Persistent LZ Compression
	DRE Compression
	Application Optimizations for file sharing, emails, web apps, enterprise apps etc.
	Proposed router should support features like SD-WAN and should be able to support SD-WAN by simply changing the software
	Should support SDN.
	Should support Next Generation Encryption features as below.
	AES-128-GCM for Authenticated Encryption
	HMAC-SHA256 for Authentication
	ECDSA-P256 for Digital Signatures
	SHA-256 for Hashing
	ECDH-P256 for Key Establishment.
	Should support Layer 3 routing protocols including RIP, OSPF, IS-IS, BGP, PBR etc.
	The router must support Over lay features like
	L2TPv3
	GRE
	MPLS
	Should have at least 4GB DRAM, with option to upgrade to 16GB.
	Should have at least and 4GB Flash, with option to upgrade up to 16GB.
	Should support Online Insertion and Removal of interface modules
	Proposed hardware should support QoS features like:
	CBWFQ
	Performance Routing
	WRED etc
	Proposed router must comply with following standards
	TIA-968-B
	CS-03
	ANSI T1.101
	ITU-T G.823, G.824
	IEEE 802.3

BILL OF MATERIAL

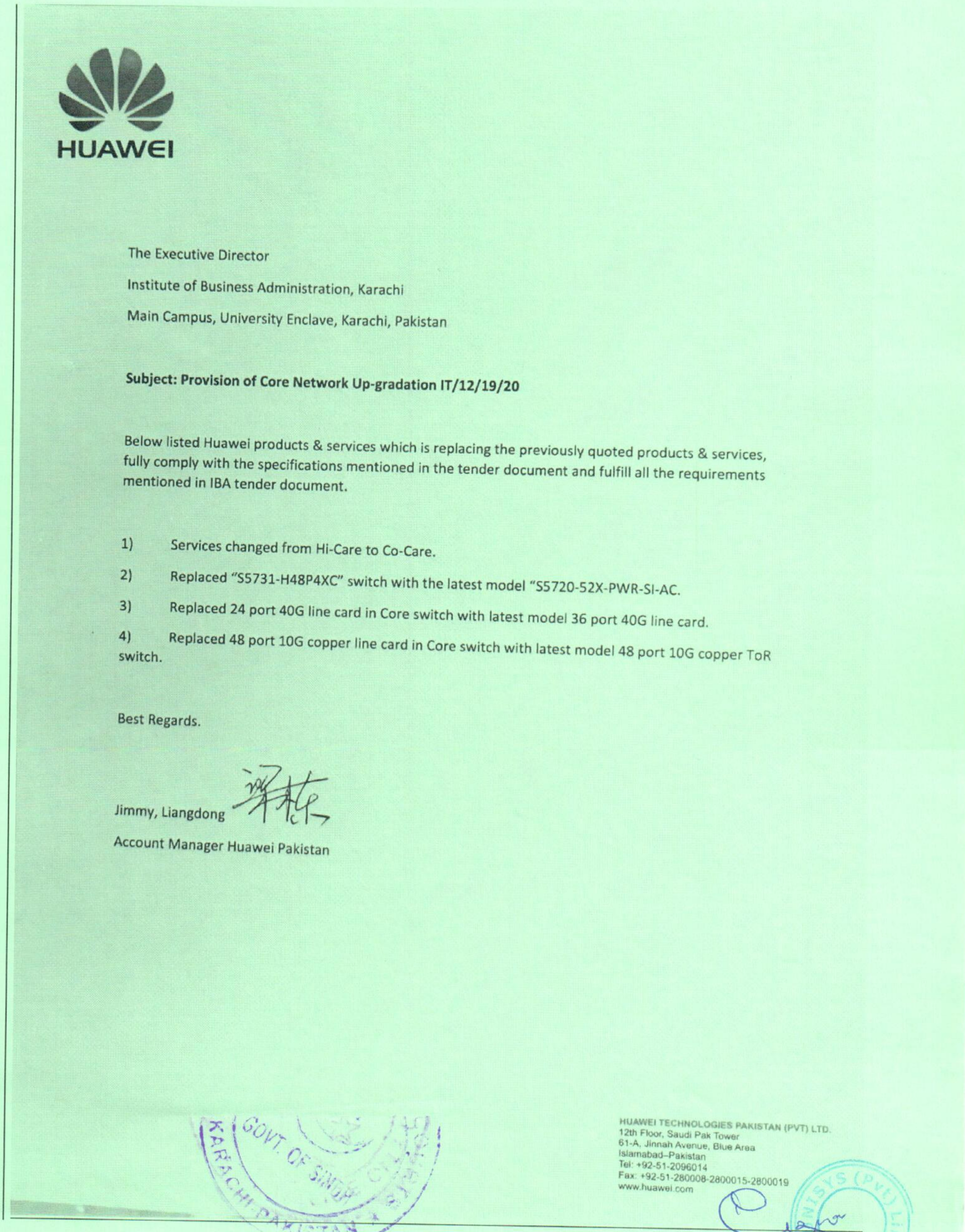
S5700 Series Ethernet Switches	
Mainframe	
S57 SI Series Mainframe	

02350DLX	S5720-52X-PWR-SI-AC	S5720-52X-PWR-SI bundle (48*10/100/1000BASE-T ports, 4*10GE SFP+ ports, PoE+, 1*500W AC power)	20
Power			
02311BXV	PAC-500WA-BE	500W AC PoE Power Module(Black, Power panel side exhaust)	20
High Speed Cable			
SFP+ High Speed Cable	**SFP+ High Speed Cable**		
02310QPR	SFP-10G-CU5M	SFP+,10G,High Speed Cable,5m,SFP+20M,CC2P0.254B(S),SFP+20M,LSFRZH For Indoor	20
CloudEngine 6800 TOR Switch			
CloudEngine 6800-Mainframe			
02351YPQ	CE6856-HI-B-B00	CE6856-48T6Q-HI Switch(48-Port 10GE RJ45,6-Port 40GE QSFP+,2*AC Power Module,2*FAN Box,Port-side Intake)	3
Software			
88035UPQ	N1-CE68LIC-CFMM	N1-CloudFabric Management SW License for CloudEngine 6800	3
88060QCW	N1-CE68CFMM-SnS1Y	N1-CloudFabric Management SW License for CloudEngine 6800 -SnS-Year	9
CloudEngine 12800 Core Switch			
Hardware			
AC Bundle			
02352GYK	CE12804SA-B6	CE12804S Bundle 6(AC/HVDC Assembly Chassis,2*MPUA-S,2*SFUG-S,2*PHD-3000WA)	1
10GBASE-X Interface Card			
03023XKA	CE-L48XS-FD	48-Port-10GE Interface Card(FD,SFP+)	1
40GBASE-X Interface Card			
03023CLT	CE-L36LQ-FD	36-Port-40GE Interface Card(FD,QSFP+)	1
Power			
02310VMA	PHD-3000WA	3000W AC&HVDC Power Module	2
Software			
88035UNT	N1-CE128LIC-CFMM	N1-CloudFabric Management SW License for CloudEngine 12800	1
88060QCA	N1-CE128CFMM-SnS1Y	N1-CloudFabric Management SW License for CloudEngine 12800 -SnS-1 Year	3
Installation Material			
02120644	WPDU3AC00	Distribution line-Basic type-PDU32-3PH-12/9-B-12*C13+9*C19-Full height vertical-With Industrial connector-Supporting mounting plate use	2
25030828	IDSPWRCBL006	Power Cable,600V/1000V,ZA-RVV,5x6mm^2,Black(5Cores:Red,Yellow,Green,Blue,Black),46A,Outdoor Cable,CE (Unit:meter)	40
SecoManager			
SecoManager Standalone Deployment Server			
02312JRC	SCM-CLU-AC-03	SecoManager Standalone AC High Configuration (2*550W AC PSU,Static Rail Kit)	1
SecoManager Software Disk			
05110JKT	SCMSWCD01-V5R19C10	SecoManager Service Software CD for V5R19C10	1
05110JKU	SCMCD01-V5R19C10	SecoManager Preinstall Software V5R19C10	1
S5700 Series Ethernet Switches			
Optical Transceiver			
10G-SFP+ Optical Transceiver			
02318169	OMXD30000	Optical Transceiver,SFP+,10G,Multi-mode Module(850nm,0.3km,LC)	16
02318170	OSX010000	Optical Transceiver,SFP+,10G,Single-mode Module(1310nm,10km,LC)	6
40GE-QSFP+Optical Transceiver			
02310MHR	QSFP-40G-iSR4	40GBase-iSR4 Optical Transceiver,QSFP+,40G,Multi-mode (850nm,0.15km,MPO)(connecting to one QSFP+ or four SFP+)	4
USG6500E			
USG6500E 1U			
02353AEK	USG6555E-AC	USG6555E AC Host(2*GE WAN+8*GE Combo+2*10GE SFP+,1 AC power)	2
Storage Module			
02312DLK	M.2-Sata240G-A	M.2 SSD,SATA 6Gb/s-240GB,Hot-Swappable	2
Power Moudle			
02312SLE	PAC60S12-AR	60W AC Power Module	2
Installation Material			
21242247	RAIL-02	Extension Guide Rail	2
Unified Security Gateway License Package			
N1 License Package			
88035WBT	N1-USG6555E-F-Lic	N1-USG6555E Foundation, Per Device	2
88060RHY	N1-USG6555E-F-SnS1Y	N1-USG6555E Foundation, SnS, Per Device, 1 Year	6
IPS-AV-URL-CS-FP License Package			
88035VYP	LIC-USG6555E-TP-3Y	Threat Protection Subscription 36 Months (Applies to USG6555E)	2

	OVS		
88035DHE	LIC-USG-E-CONTENT	Content Security Group Function	2
USG6500E			
Subassembly | Accessories,USG6500E,Main Euquipment			
USG6500E 1U			
02353AFX	USG6525E-AC	USG6525E AC Host(2*GE WAN+8*GE Combo+2*10GE SFP+,1 AC power)	2
Storage Module			
02312DLK	M.2-Sata240G-A	M.2 SSD,SATA 6Gb/s-240GB,Hot-Swappable	2
Power Moudle			
02312SLE	PAC60S12-AR	60W AC Power Module	2
Installation Material			
21242247	RAIL-02	Extension Guide Rail	2
Unified Security Gateway License Package			
N1 License Package			
88035WBR	N1-USG6525E-F-Lic	N1-USG6525E Foundation, Per Device	2
88060RHW	N1-USG6525E-F-SnS1Y	N1-USG6525E Foundation, SnS, Per Device, 1 Year	6
IPS-AV-URL-CS-FP License Package			
88035VYM	LIC-USG6525E-TP-3Y-OVS	Threat Protection Subscription 36 Months (Applies to USG6525E)	2
88035DHE	LIC-USG-E-CONTENT	Content Security Group Function	2
AR6100 Series Enterprise Routers			
AR6100 Mainframe and Module			
02352UNK	AR6140-9G-2AC	AR6140-9G-2AC AC host, 5*GE RJ45, 4*GE SFP, 1*USB 3.0, 4*SIC	2
Software			
Data Package Licenses			
81401309	LAR0DATAE10	AR6100 Value-Added Data Package	2
Security Package Licenses			
81401315	LAR0SECE10	AR6100 Value-Added Security Package	2
S5720-52X-PWR-SI-AC(C13_Britain)_Access Switch			
S5700 Series Ethernet Switches			**20**
88134UGQ-4NS	02350DLX_88134UGQ-4NS_36	S5720-52X-PWR-SI bundle_Co-Care Standard S5720-SI-52X-PWR_36Month(s)	20
CE6856-48T6Q-HI(PDUC13_Europe)_Server Farm Switch			
CloudEngine 6800 TOR Switch			**3**
CE12804S(PDUC19_China/Europe/America/Korea) V200R019_Core Datacenter Switch			
CloudEngine 12800 Core Switch			**1**
88134UHD-248	02352GYK_88134UHD-248_36	CE12804S Bundle 6(AC/HVDC Assembly Chassis,2*MPUA-S,2*SFUG-S,2*PHD-3000WA)_Co-Care Premier CE12804S Chassis_36Month(s)	1
88134UHD-278	03023CLT_88134UHD-278_36	36-Port-40GE Interface Card(FD,QSFP+)_Co-Care Premier CE12800 36-Port-40GE Interface Card(FD,QSFP+)_36Month(s)	1
88134UHD-281	03023XKA_88134UHD-281_36	48-Port-10GE Interface Card(FD,SFP+)_Co-Care Premier CE12800 48-Port-10GE Interface Card(FD,SFP+)_36Month(s)	1
SecoManager HW(PDUC13_Europe) V500R019_Firewall NMS			
SecoManager			**1**
88134UHD-2JQ	02312JRC_88134UHD-2JQ_36	SecoManager Standalone AC High Configuration (2*550W AC PSU,Static Rail Kit)_Co-Care Premier RH2288/2288H_36Month(s)	1
USG6555E-AC(PDUC13_Europe) V600R007_Internet Firewall			
USG6500E			**2**
88134UHD-46H	02353AEK_88134UHD-46H_36	USG6555E AC Host(2*GE WAN+8*GE Combo+2*10GE SFP+,1 AC power)_Co-Care Premier USG6555E_36Month(s)	2
USG6525E-AC(PDUC13_Europe) V600R007_DC Firewall			
USG6500E	**USG6500E**		**2**
88134UHD-46L	02353AFX_88134UHD-46L_36	USG6525E AC Host(2*GE WAN+8*GE Combo+2*10GE SFP+,1 AC power)_Co-Care Premier USG6525E_36Month(s)	2
AR6140_9G_2AC(PDUC13_Europe)_internet router			
AR6100 Series Enterprise Routers			**2**
88134UHD-47W	02352UNK_88134UHD-47W_36	AR6140-9G-2AC AC host, 5*GE RJ45, 4*GE SFP, 1*USB 3.0, 4*SIC_Co-Care Premier AR6140-9G-2AC_36Month(s)	2

Part Number	Description	Qty
ISR4331/K9	Cisco ISR 4331 (3GE,2NIM,1SM,4G FLASH,4G DRAM,IPB)	2
CON-SNTP-ISR4331K	SNTC-24X7X4 Cisco ISR 4331 (2GE,2NIM,1SM,4G FLASH,4G	2
SL-4330-IPB-K9	IP Base License for Cisco ISR 4330 Series	2
SL-4330-UC-K9	Unified Communication License for Cisco ISR 4330 Series	2
PVDM4-64	64-channel DSP module	2

PWR-4330-AC	AC Power Supply for Cisco ISR 4330	2
CAB-ACU	AC Power Cord (UK), C13, BS 1363, 2.5m	2
MEM-FLSH-4G	4G Flash Memory for Cisco ISR 4300 (Soldered on motherboard)	2
MEM-43-4G	4G DRAM (1 x 4G) for Cisco ISR 4300	2
NIM-BLANK	Blank faceplate for NIM slot on Cisco ISR 4400	2
SM-S-BLANK	Removable faceplate for SM slot on Cisco 2900,3900,4400 ISR	2
CUBE-T-STD	CUBE - 1 Standard Trunk Session License	140
CON-ECMU-CUBETSTD	SWSS UPGRADES CUBE Standard Trunk Single Session - 1 S	140
NIM-4FXO	4-port Network Interface Module - FXO (Universal)	2
SISR4300UK9-166	Cisco ISR 4300 Series IOS XE Universal	2



HUAWEI

The Executive Director

Institute of Business Administration, Karachi

Main Campus, University Enclave, Karachi, Pakistan

Subject: Provision of Core Network Up-gradation IT/12/19/20

Below listed Huawei products & services which is replacing the previously quoted products & services, fully comply with the specifications mentioned in the tender document and fulfill all the requirements mentioned in IBA tender document.

1) Services changed from Hi-Care to Co-Care.

2) Replaced "S5731-H48P4XC" switch with the latest model "S5720-52X-PWR-SI-AC.

3) Replaced 24 port 40G line card in Core switch with latest model 36 port 40G line card.

4) Replaced 48 port 10G copper line card in Core switch with latest model 48 port 10G copper ToR switch.

Best Regards.

Jimmy, Liangdong

Account Manager Huawei Pakistan

HUAWEI TECHNOLOGIES PAKISTAN (PVT) LTD.
12th Floor, Saudi Pak Tower
61-A, Jinnah Avenue, Blue Area
Islamabad–Pakistan
Tel: +92-51-2096014
Fax: +92-51-280008-2800015-2800019
www.huawei.com

GOVT. OF SINDH
KARACHI PAKISTAN

NISYS (Pvt) Limited

2.2 The "Supplier" is committed to provide three (3) years' comprehensive onsite warranty (Manufacturer) with parts and free services from the date of delivery.

2.3 Standard sets of General toolkit/ accessories supplied with equipment shall be provided by the M/s IBL Unisys (Pvt) Ltd with no additional cost.

2.4 A liquidity damages in the event of delay in delivery at supplier fault, the supplier shall inform the purchaser before expiry of such period giving reasons or justification for delay. However, purchaser reserves the right to take following actions:

i. Evaluate the request for extension in delivery period as per its merit and may consider extension in delivery period or otherwise.
ii. May cancel the contract.
iii. Liquidated damages (if imposed) will be recovered at the rate of up to 2% per month and shall not exceed 10% of the total value of the contract.

2.5 Performance Security 5% of total amount of Purchase Order will be provided by the M/s IBL Unisys (Pvt) Ltd.

2.6 Stamp duty 0.35% (for stamp duty amount converted in PKR by Rs. 156 per US$) against total value of Purchase Order will be levied accordingly and born by the successful bidder.

2.7 If any tax exemptions, reductions, allowances or privileges may be available to the Supplier in the Pakistan, the IBA shall use its best efforts to enable the Supplier to benefit from any such tax savings to the maximum allowable extent.

2.8 Applicable withholding taxes, rates, duties, etc. shall be deducted from supplier payments.

2.9 No increase in the value of above-mentioned items will be accepted on account of either unit price, total price, any or all other charges, duties, taxes, scope of supply and or any other head of account shall be allowed.

Article III
LETTER OF CREDIT (LC)

3.1 LC charges (client-side) and Import Duties & Taxes (where applicable) will be borne by IBA, Karachi. However, the successful bidder will pay import duties & taxes and bill separately to IBA as reimbursable expenses upon presentation of proof of payment.

3.2 M/s IBL Unisys (Pvt) Ltd should clearly indicate the name and full address of their principals/authorized distributor in whose favour LC shall be opened. In case of distributer, the authorization certificate from Principal for specific bid shall be obtained.

Article IV
BIDDER'S RESPONSIBILITY

4.1 M/s IBL Unisys (Pvt) Ltd shall be responsible for transportation of complete consignment to IBA, Karachi premises. This would include cost of labour for unloading consignment to the designated warehouse. Labour will be provided by the bidder.

GOVT. OF SINDH KARACHI-PAKISTAN OURTS

UNISYS (PVT) LIMI

Article V
MODE OF DELIVERIES

5.1 Supply will be delivered at IBA Store Main Campus University Enclave Karachi within 08 weeks of establishment of LC.

5.2 If M/s IBL Unisys (Pvt) Ltd fails to timely deliver items/services as per BoQ , IBA, Karachi reserves the right to penalize and may also terminate the contract.

Article VI
TERMS OF PAYMENT

6.1 All payments will be made through LC in the name of Principal / authorized distributor.

6.2 70% of LC Value will be released on arrival at Karachi Port (LC at sight).

6.3 Remaining 30% of LC value will be released on issuance of Acceptance Certificate after delivery of goods at IBA, Karachi premises.

Article VII
FORCE MAJEURE

7.1 M/s IBL Unisys (Pvt) Ltd shall not be held liable in the event of their failure to comply with the delivery schedule of the ordered items(s) for reasons of Force Majeure including to war and other instabilities invasion, act of foreign enemies, embargo, civil war etc.

Article VIII
ARBITRATION

8.1 In case of any dispute, difference or and question which may at any time arise between the parties hereto or any person under them, arising out in respect of this letter of intent or this subject matter thereof shall be referred to the Registrar of the IBA for arbitration/settling of the dispute, failing which the decision of the court law in the jurisdiction of Karachi binding to the parties. The Arbitration proceedings will be governed by the Arbitration Act, 1940 and the Substantive and procedural law of Pakistan. The venue shall be Karachi.

Article IX
TERMINATION

9.1 If M/s IBL Unisys (Pvt) Ltd fails to timely deliver items/services as per BoQ , IBA, Karachi reserves the right to penalize and may also terminate the contract.

Article X
INDEMNITY

10.1 "THE SUPPLIER" in its individual capacity shall indemnify and keep IBA and any person claiming through IBA fully indemnified and harmless from and against all damages, cost and expenses caused to or incurred by "THE SUPPLIER", as a result of any defect in the title of IBA or any fault, neglect or omission by the "THE SUPPLIER" which disturbs or damage the reputation, quality or the standard of services provided by "IBA" and any person claiming through the IBA.

GOVT. OF SINDH
KARACHI-PAKISTAN

Article XI
NOTICE

11.1 Any notice given under this AGREEMENT shall be sufficient if it is in writing and if sent by courier or registered mail.

11.2 If the Agreement or encounters conditions impeding timely performance of any of the obligations, under the contract, at any time, the Supplier shall, by the written notice served on the IBA promptly indicating the facts of the delay, its likely duration and its cause(s).As soon as practicable after receipt of such notice, the IBA shall evaluate the situation and may, at its exclusive discretion, without prejudice to any other remedy it may have, by written order served on the "Supplier", extend the Agreement's time for performance of its obligations under the Agreement

Article XII
SEVERABILITY

12.1 If any terms covenant or condition of this agreement shall be deemed invalid or unenforceable in a court of law or equity, the remainder of this agreement shall be valid & enforced to the fullest extent permitted by prevailing law.

Article XIII
WARRANTY

13.1 The "Supplier" is committed to provide three (3) years' comprehensive onsite warranty (Manufacturer) with parts and free services from the date of delivery.

Article XIV
OWNERSHIP

14.1 The ownership of all products and services rendered under any contract arising as a result of this tender will be the sole property of IBA, Karachi.

Article XV
SECRECY & CONFIDENTIALITY

15.1 M/s IBL Unisys (Pvt) Ltd will be responsible to maintain secrecy/ confidentiality of information /Data shared during all stages of Contract.

Article XVI
DEFAULT

16.1 If M/s IBL Unisys (Pvt) Ltd fails to timely deliver items/services as per BoQ , IBA, Karachi reserves the right to penalize and may also terminate the contract.

Article XVII
LIQUIDATED DAMAGES

17.1 A liquidity damages in the event of delay in delivery at supplier fault, the supplier shall inform the purchaser before expiry of such period giving reasons or justification for delay. However, purchaser reserves the right to take following actions:

iv. Evaluate the request for extension in delivery period as per its merit and may consider extension in delivery period or otherwise.

v. May cancel the contract.

vi. Liquidated damages (if imposed) will be recovered at the rate of up to 2% per month and shall not exceed 10% of the total value of the contract.

GOVT. OF SINDH
PAKISTAN

UNISYS (Pvt) Limi

Article XVIII
DELIVERY PERIOD

18.1 Delivery period 08 weeks from the LC establishment.

Article XXI
INTEGRITY PACT

19.1 The intention not to obtain the procurement of any Contract, right, interest, privilege, or other obligation or benefit from the IBA or any administrative or financial offices thereof or any other department under the control of the IBA through any corrupt practice(s).

19.2 Without limiting the generality of the forgoing the M/s IBL Unisys (Pvt) Ltd, represents and warrants that it has fully declared the charges, fees, commission without any taxes, levies etc, paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within the IBA directly or indirectly through any means any commission, gratification, bribe, gifts, kickback whether described as consultation fee or otherwise, with the object of obtaining or including the procurement or service contract or order or other obligations whatsoever from the IBA, except that which has been expressly declared pursuant hereto.

19.3 M/s IBL Unisys (Pvt) Ltd, accepts full responsibility and strict liability for making any false declaration/statement, not making full disclosure, misrepresenting facts or taking any action likely to degrade the purpose of declaration, representation and warranty. It agrees that any contract/order obtained aforesaid shall without prejudice to any other right & remedies available to the IBA under any law, contact, or other instrument, be stand void at the discretion of the IBA.

19.4 Notwithstanding any right and remedies exercised by the IBA in this regard, M/s IBL Unisys (Pvt) Ltd, agrees to indemnify the IBA for any loss or damage incurred by it on account of its corrupt business practice & further pay compensation to the IBA in any amount equivalent to the loss of any commission, gratification, bribe, gifts, kickback given by the M/s IBL Unisys (Pvt) Ltd, as aforesaid for the purpose of obtaining or inducing procurement or other obligation or benefit in whatsoever from the IBA.

Article XIV
MISCELLANEOUS

20.1 Any addition & alteration(s) made for item(s) as required by IBA on the basis of sample or in course of the supplies which entail extra time & labor and material on part of the supply, shall not be charged separately/extra on 'Quantum Merit' basis before & on final material handed over to the "IBA.

20.2 The terms and conditions of the AGREEMENT have been read over to the parties which they admit to be correct and abide by the same.

20.3 The validity of the contract will be effective from the date of issue of Purchase Order.

20.4 All terms and conditions of tender vide # IT/12/19-20 will be the integral part of this agreement and can't be revoked.

GOVT. OF SINDH
COURTS

UNISYS (Pvt) Limited

IN WITNESS WHEREOF both the parties hereto have set & subscribed their respective hands to this agreement at Karachi on the date as mentioned above.

Dr. Mohammad Asad Ilyas
Registrar
Former Chairperson Accounting & Law Department
Institute of Business Administration (IBA).
Karachi, Pakistan

“IBA”
NAME: Dr. Muhammad Asad Ilyas
CNIC # 42301-4497722-9

Address:
Registrar, Institute of Business
Administration Main Campus
University Enclave, Karachi

IBL UNISYS (Pvt) Limited

M/S IBL Unisys (Pvt) Ltd
NAME: Rizwan Ahmed
CNIC # 42101-0901274-1

Address:
2nd Floor, One IBL Center, Plot # 1,
Block 7 & 8. DMMCHS, Tipu Sultan Road
Off Shahrah-e-Faisal, Karachi

3.

“IBA”
NAME: Syed Fahad Jawed

CNIC # 42201-9125136-3

Address:
Head of Procurement
Institute of Business
Administration Main Campus
University Enclave, Karachi

for,

IBL UNISYS (Pvt) Limited

4.

M/s IBL Unisys (Pvt) Ltd
NAME: Mian Haseeb Tariq

CNIC # 54400-7500435-5

Address:
2nd Floor, One IBL Center, Plot # 1,
Block 7 & 8. DMMCHS,
Tipu Sultan Road,
Off Shahrah-e-Faisal, Karachi

Focal Person IBA

S.M. Wajeeh Zaidi
Head of ICT

GOVT. OF SINDH